Vol.2009-CSEC-46 No.39
2009/7/3

企業における情報セキュリティ基準と対策の関係に関する一考察

沼田 晋作[†1] 柴田 賢介[†1]
岡崎 聖人[†1] 高橋 克巳[†1]

現在の企業における情報セキュリティ対策に，ISMS 適合性評価制度が与える影響は少なくないと考えられる．しかし，ISMS 適合性評価制度によって評価を受けた企業においても情報セキュリティ対策には各種課題が残されている．本論文では、企業における情報セキュリティ対策の現状調査を実施し，その結果から ISMS 適合性評価制度の影響下にある企業において，対策の有効性測定の実施率が 29%であった等の PDCA サイクルの断絶が見られたことを示し，その原因の 1 つとして管理者におけるインシデント等の発生頻度情報の利用に課題があることを述べる．

A study of relation between information security criteria and controls in enterprise

Shinsaku Numata ,[†1] Kensuke Shibata ,[†1]
Masato Okazaki [†1] and Katsumi Takahashi[†1]

It is thought that the influence that the ISMS conformity assessment scheme has on the information security controls in a enterprise is not a little. However, various problems have been left in the information security controls in the enterprise that receives the evaluation by the ISMS conformity assessment scheme. In this thesis, the current situation survey of the information security controls in the enterprise is executed, and it shows that the rupture at the PDCA cycle,29% at the execution rate of the effectiveness measurement of controls etc.And the one of the causes is problem for not using incidence frequency information of incident.

1. はじめに

近年，インターネット等への情報流出事件が発生し，社会問題となっている．このため，企業では情報資産を情報セキュリティインシデントから守るために，各種情報セキュリティ対策を導入している．また，情報セキュリティに関する基準も複数存在し，それらを活用した情報セキュリティ対策の実施を行う企業も存在する．そして，その情報セキュリティ基準の 1 つとして，JIS Q 27001:2006[1)] が存在する．

JIS Q 27001:2006 は，日本の ISMS 適合性評価制度において活用される情報セキュリティ基準である[2)]．ISMS 適合性評価制度とは，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う組織のマネジメントシステムが認証基準に適合するかを第三者が評価する制度である．この評価に合格すると，ISMS 認証取得組織織となることができ，対外的な情報セキュリティの信頼性を確保することができる．[2)] しかし，この JIS Q 27001:2006 に適合していると判断された ISMS 認証取得組織において，情報漏洩等の情報セキュリティインシデントの発生や，ISMS 実施における業務負荷の増大などの各種課題点が指摘[3)] されるようになってきている．

このため本研究では，企業における情報セキュリティ対策の現状について，情報セキュリティ対策製品がどの様な動機で導入が決定され，どの様なインシデントが想定されて製品が選定され，どの様に運用されているのか等，企業における情報セキュリティの PDCA サイクルに関する調査を行った．それらの調査結果と ISMS 適合性評価制度で利用される情報セキュリティ基準である JIS Q 27001:2006 とを比較することで，企業における情報セキュリティ基準と情報セキュリティ対策の関係に関する考察を述べ，課題点を明らかにする．

本稿では，今回実施した調査の結果を紹介し，その結果から考えられる企業の情報セキュリティの課題点を述べる．まず，2 章にて実施した調査の概要を述べる．そして 3 章にて調査結果を示す．4 章にて調査結果を元に企業の情報セキュリティ対策の現状に関する考察を述べる．最後に，5 章にてまとめを述べ 6 章で今後の課題を述べる．

2. 調査概要

本章では，本研究で行った調査の概要を述べる．

†1 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

Vol.2009-CSEC-46 No.39
2009/7/3

2.1 調 査 内 容

本調査では企業における情報セキュリティ対策の現状について調査する．今回取りあげた情報セキュリティ基準である JIS Q 27001:2006 では，情報セキュリティ対策を PDCA サイクルに基づいて実施する事を推奨している．このため，本調査では企業における情報セキュリティ対策製品の導入における PDCA サイクルの実施状況を調査することとした．

2.2 調 査 方 式

調査は Web アンケート方式とした．回答者は Web ブラウザでインターネット上の Web サーバにアクセスし，表示される設問に対し回答する．回答は選択肢の選択，数値の入力，自由記述のいずれかで行う．選択肢の選択はマウスを用いて行い，数値の入力や自由記述はキーボードを使用して回答を行えるように Web ページを作成した．

2.3 調査対象者

本調査では，次の条件を全て満たす人を対象として Web アンケートを行った．

- 毎日 PC を使用する業務を行う
- 現在の企業に 3 年以上勤務している
- 企業における情報セキュリティ管理者の立場にある
- 情報セキュリティ対策製品の導入を行ったことがある

今回はこれらを条件とし，年齢や性別，企業規模等については制限を設けず，1741 人の情報セキュリティ管理者を対象にした調査を実施した．本調査では，企業の情報セキュリティ対策の策定に関与する者を，情報セキュリティ管理者とした．

2.4 質問項目概要

アンケートの質問項目は，回答者自身の勤務する企業の情報セキュリティ対策製品の導入にまつわる，PDCA サイクルの実施状況に関する質問項目とした．

質問項目のうち，本論文で着目する PDCA サイクルの実施状況についての質問項目を表 1 に示す．また，表 1 に記載した質問項目で明らかになる情報のうち,「情報セキュリティ対策製品 (Q1)」「情報資産 (Q2)」「情報セキュリティ対策製品導入の動機 (Q6)」「インシデント (Q7)」「脆弱性 (Q11)」「脅威 (Q12)」それぞれについて，図 1 の様な関係があることを意識させた質問設計とした．

2.5 質問項目詳細

本節では，2.4 節で述べた質問項目についての詳細な説明を述べる．

2.5.1 情報セキュリティ対策製品導入の動機（JIS Q 27001:2006 の影響の有無）

本調査では，情報セキュリティ対策製品導入の動機を調査する質問項目を設けた．この結果を用いて，その企業の情報セキュリティ対策が，情報セキュリティ基準 JIS Q 27001:2006 の影響を受けているか，そうでないかを調査し，回答者を JIS Q 27001:2006 の影響下にある管理者とそれ以外の管理者の 2 つのグループに分類した．

この分類によって，情報セキュリティ基準 JIS Q 27001:2006 で述べられていることと，JIS Q 27001:2006 の影響下にある管理者の回答を比較することが可能となり，JIS Q 27001:2006 で述べられている内容が，企業においてどの程度実施されているかを把握することが可能となる．

さらに，JIS Q 27001:2006 の影響下にある企業と，そうでない企業を比較することで，情報セキュリティ基準が企業の対策に与える影響を測ることが可能となる．

選択肢として「ISMS 認証取得のため」「Pマーク取得」「法令・規制等の遵守」「業界自主取組み」「自社情報セキュリティ事故（インシデント）の発生」「他社情報セキュリティ事

表 1 PDCA サイクルの実施状況把握のための質問項目

質問番号	質問内容
Q1	情報セキュリティ対策製品
Q2	情報セキュリティ対策製品が守っている情報資産
Q6	情報セキュリティ対策製品導入の動機
Q7	発生しうるインシデントの特定
Q10	インシデント発生頻度目標の設定
Q11	脆弱性の特定
Q12	脅威の特定
Q20	対策製品の使用割合把握
Q22	インシデント発生検知手順策定
Q23	実インシデント発生頻度把握
Q24	インシデント発生頻度目標の達成確認
Q28	ユーザ意見収集方法策定
Q31	ユーザ意見の適用
Q33	インシデント発生情報の適用

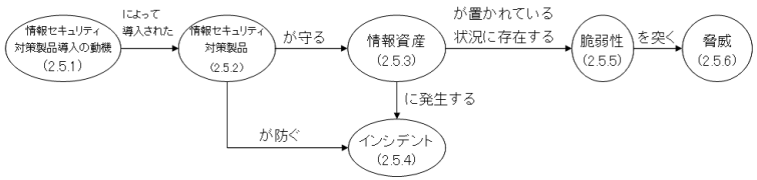

図 1 アンケートにおける質問項目の関係 (図中番号は本論文の節番号)

表 2 製品分類

製品分類	製品例
メール関係	メールフィルタ，メールアーカイヴ，メール暗号化
Web 関係	Web フィルタ，オンラインストレージ
電子ファイル関係	電子ファイルアクセス制御 (DRM/持ち出し制御)，コンテンツフィンガープリンティング，ファイル暗号化，機密情報検索
記録媒体関係	HDD 暗号化，セキュアな外部記録媒体，データ完全消去
システムユーザ ID 関係	ID 管理，ユーザ認証強化（PKI），ユーザ認証強化（PKI 以外），証跡管理
ネットワークセキュリティ関係	社内 NW セキュリティ（検疫 NW,NBAND, 脆弱性診断），社外 NW セキュリティ(Firewall,UTM,WAF)
ストレージ関係	データバックアップ
物理セキュリティ関係	入退室管理，持ち出し管理

故（インシデント）の発生」「既存セキュリティ対策製品の入れ替え」「取引先からの要請」「ある製品を使うことが既に決められていた」「わからない」という選択肢を準備し，それらの中から選ぶように質問項目を作成した．その中で「ISMS 認証取得のため」を選択した回答者を，JIS Q 27001:2006 の影響下にある回答者と判断することとした．

2.5.2 情報セキュリティ対策製品

本調査では，企業に導入された情報セキュリティ製品を調査する質問項目を設けた．回答者に情報セキュリティ対策製品の一覧を表示し，その中から実際に導入された情報セキュリティ対策製品を１つ回答してもらうこととした．

この際に，特定の情報セキュリティ対策製品に回答者の選択結果が偏ることが考えられた．選択結果に偏りが生じた場合，調査結果に特定の情報セキュリティ対策製品の影響が出てしまうことが考えられた．このため，表 2 のようなカテゴリによる製品分類を行い，カテゴリ毎に回答者数が平均的になる様に，回答者の選定（スクリーニング）を実施した．

2.5.3 情報セキュリティ対策製品が守っている情報資産

2.5.2 節にて回答者が選択した情報セキュリティ対策製品が，回答者自身の扱うどの様な情報を守るために導入されたかについて質問項目を設けた．選択肢として「個人情報」「営業秘密」「その他重要情報」を提示し，一つを回答してもらうこととした．

2.5.4 情報セキュリティ製品が防止しているインシデント

2.5.2 節にて回答者が選択した情報セキュリティ対策製品が，2.5.3 節にて選択した回答者自身が扱う情報資産に起こりうるどの様なインシデントを防止するために導入されたかについて調査した．選択肢として,「情報漏洩」「情報改竄」「情報へアクセス出来なくなる」「情報アクセス履歴が追えなくなる」「不正利用」「わからない」のいずれかから１つを回答してもらうこととした．

2.5.5 情報資産に存在している脆弱性

2.5.3 節にて回答者が選択した情報資産に存在する脆弱性の中で，2.5.2 節にて選択した情報セキュリティ対策製品がカバーする脆弱性を調査する質問項目を設けた．選択肢としては，電子ファイルが格納されている機器が設置されている部屋等,「電子ファイルが格納されているサーバ、アプリケーション」「電子ファイルを使用するクライアント PC」「電子ファイルをやりとりするネットワーク」「電子ファイルをやりとりする媒体」「電子ファイル自体」「情報セキュリティの欠陥（脆弱性）はなかった」「わからない」，として 1 つを回答してもらうこととした．

2.5.6 情報資産に存在している脆弱性を突く脅威

2.5.5 節で回答として得た脆弱性を突く脅威を調査する質問項目を設けた．選択肢としては,「内部の人間の過失による操作・行動」「内部の人間の故意による操作・行動」「外部の関係者の過失による操作・行動」「外部の関係者の故意による操作・行動」「第三者の過失による操作・行動」「第三者の故意による操作・行動」「ワーム・ウィルス等の悪意のあるプログラムの動作」「プログラムのバグによる誤動作」「その他（経年劣化や自然災害などによる故障等)」「わからない」，として 1 つを回答してもらうこととした．

2.5.7 情報セキュリティ対策製品の運用状況

導入された情報セキュリティ対策製品の，運用状況を調査する質問項目を設けた．情報セキュリティ対策製品が実際に使用されているかだけでなく，その情報セキュリティ対策製品の実施割合をどの様に把握しているか，インシデントが発生したときにどの様な対処を取ることになっているか，なども含めて導入された情報セキュリティ対策製品の運用状況を調査した．具体的な質問項目としては,「インシデント目標発生頻度」「対策実施率把握方法・管理方法」「インシデント把握方法・管理方法」「インシデント発生有無」「クレーム収集ルートの有無」「インシデント発生頻度の目標との比較の有無」「クレーム情報活用の有無」「収集情報活用の有無」を調査した．

3. 調 査 結 果

本章では，2 章で述べたアンケートを実施し得られた結果を，情報セキュリティ対策における PDCA サイクルの実施状況として示す．

Vol.2009-CSEC-46 No.39
2009/7/3

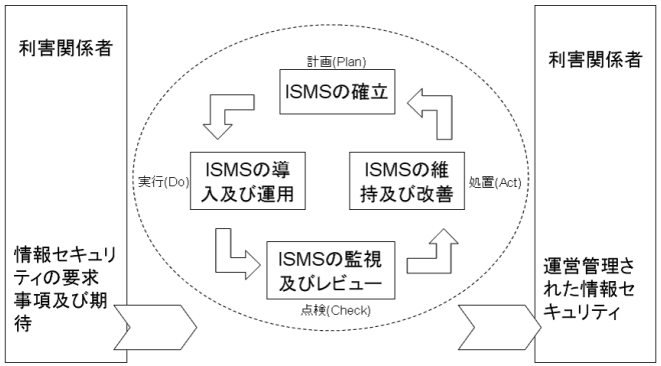

図 2 JIS Q 27001:2006 における PDCA サイクルと利害関係者の位置づけ (出典：JIS Q 27001:2006 *0.2.2* 図 1)

3.1 実施した質問項目の PDCA サイクルへの分類

調査結果を PDCA サイクルに分類するためには，PDCA サイクルの定義が必要である．本研究では ISMS 適合性評価制度の審査で使用される JIS Q 27001:2006 の項目で述べられている内容を使用し，アンケート結果を PDCA の各プロセスに分類した．図 2 に示すように JIS Q 27001:2006 では，PDCA それぞれの活動を同基準の *0.2.2*[⋆1]の図，および *4.2*「ISMS の確立及び運営管理」にて定義している．[1)]

表 1 に示す我々の実施したアンケートの各質問項目を，JIS Q 27001:2006 の 4.2 節「ISMS の確立及び運営管理」にて定義された PDCA の内容を元に分類した．JIS Q 27001:2006 では *4.2.1* の ISMS の確立で P(Plan) を，*4.2.2* の「ISMS の導入及び運用」で D(Do) を，*4.2.3* の「ISMS の監視及びレビュー」で C(Check) を，*4.2.4* の「ISMS の維持及び改善」で A(Action) をそれぞれ定義している．この内容に基づいて質問項目を取りあげ，それぞれ企業における PDCA サイクルの認識状況とした．この分類を表 3 に示す.

3.2 調査結果データ

3.2.1 JIS Q 27001:2006 影響下の管理者数

まずは，JIS Q 27001:2006 の影響下にある管理者とそうでない管理者の数を述べる．

⋆1 本論文の節番号等と区別するため，本論文中では JIS Q 27001: 2006 内の節番号等をイタリックフォントで表記する．

表 3 PDCA サイクルとの対応付け

サイクル名	対応 JIS Q 27001:2006 の項目番号と概要	質問内容 (質問番号)
P(Plan)	*4.2.1 c) 2)* リスク受容レベルの特定	インシデント発生頻度目標の設定 (Q10)
	4.2.1 d) 2) 資産に対する脅威の特定	脅威の特定 (Q12)
	4.2.1 d) 3) 脅威に付け込む脆弱性の特定	脆弱性の特定 (Q11)
	4.2.1 d) 4) CIA の喪失が資産に及ぼす影響の特定	発生しうるインシデントの特定 (Q7)
D(Do)	*4.2.2 c)* 管理策の実施	対策製品の使用割合把握 (Q20)
	4.2.2 h) インシデントへの対応手順の実施	インシデント発生検知手順策定 (Q22)
C(Check)	*4.2.3 a) 2)* インシデントの特定	実インシデント発生頻度把握 (Q23)
	4.2.3 b) ISMS のレビューと利害関係者からのフィードバック	ユーザ意見収集方法策定 (Q28)
	4.2.3 c) 管理策の有効性の測定	インシデント発生頻度目標の達成確認 (Q24)
A(Action)	*4.2.4 b)* 自他組織のセキュリティ経験の適用	ユーザ意見の適用 (Q31)
		インシデント発生情報の適用 (Q33)

アンケートでは 1741 人へ回答を依頼し，有効回答として 357 人を得ることが出来た．この有効回答の中で，製品の導入動機が「ISMS 認証取得のため」と回答した回答者は 37 人であり，その他の動機を選択した回答者は，320 人であった．このため以後は，前者を JIS Q 27001:2006 の影響下にある企業の管理者として扱う.（以後「ISMS 影響下の管理者」と記述する）そして，後者を JIS Q 27001:2006 以外の影響下にある企業の管理者として扱い，「非 ISMS 影響下の管理者」と記述する．

3.2.2 PDCA 実施状況

3.1 節にて PDCA それぞれの各プロセスに分類した質問項目において,「実施している」と回答した管理者の割合を PDCA 実施率とし，本調査の目的である企業における情報セキュリティの PDCA 実施状況とする．この PDCA の各プロセスの実施状況を図 3 に示す.

PDCA サイクルのそれぞれについて，実施率が高い項目と，低い項目が見られた．全体の傾向として，PDCA の P(Plan) や D(Do) については高く，C(Check) や A(Action) については低い傾向となった.

実施率が最も高かった項目は，PDCA サイクルでは P(Plan) にあたる,「発生しうるインシデントの特定 (Q7)」(JIS Q 27001:2006 *4.2.1 d) 4)*) で，100%の実施率であった.

しかし，P(Plan) の中でも実施率が低い項目が存在した．リスク受容可能レベルの設定 (JIS Q 27001:2006 *4.2.1 c)*) に当たる「インシント発生頻度目標の設定 (Q10)」である．この内容を実施していると回答したのは 59%であるという結果となった.

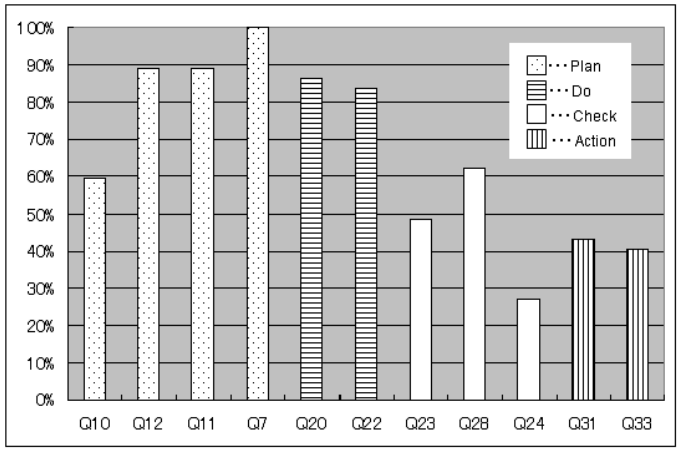

図 3 PDCA 各サイクルにおける実施率 (ISMS 影響下にある管理者．n=37)

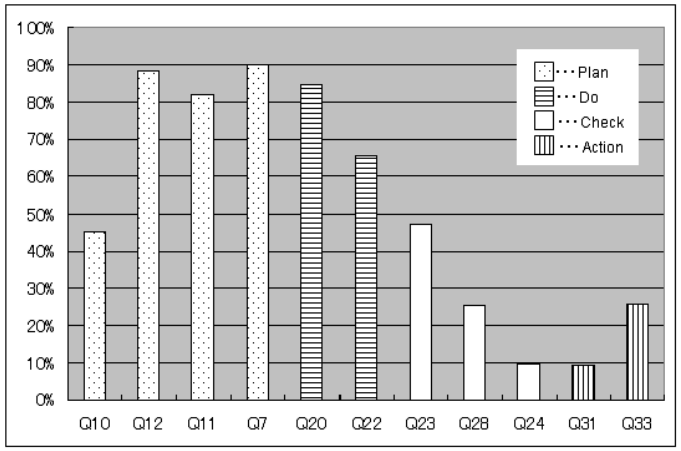

図 4 PDCA 各サイクルにおける実施率 (非 ISMS 影響下にある管理者．n=320)

他にも，C(Check) にあたる「実インンシデントの発生頻度把握 (Q23)」(JIS Q 27001 *4.2.3 b)*) の実施率は 49%であった．有効性の測定 (JIS Q 27001 *4.2.3 c)*) にあたる「インシデント発生頻度目標の達成確認 (Q24)」の実施率は 27%であった．

A(Action) にあたる「インシデント発生情報の適用 (Q33)」(JIS Q 27001 *4.2.4 b)*) については，41%の実施率であり「ユーザ意見の適用 (Q31)」(JIS Q 27001 *4.2.4 b)*) も似たような実施率である 43%であった．

同様に，非 ISMS 影響下にある管理者の回答結果を図 4 に示す．全ての項目について ISMS 影響下にある管理者の実施割合を下回っているが，全体的に似たような傾向を示している．

4. 考　　察

本章では，3 章にて示した結果を基に，企業の情報セキュリティ対策の現状についての考察を述べる．

4.1 JIS Q 27001:2006 の与える影響

まず，図 3 と図 4 を比較して，ISMS 影響下にある管理者の回答の方が，非 ISMS 影響下にある管理者の回答と比較して PDCA の各プロセスにおける実施率が高かった事が分かる．特に PDCA サイクルのうち C と A について大きな差が見られた．これは，ISMS 適合性評価制度を経る中で，情報セキュリティに対する意識の向上などの影響が与えられたことが理由と考えられる．平成 19 年 3 月に財団法人ニューメディア開発協会が実施した，「ISMS の維持管理における実態調査」[3] において，「ISMS 認証取得によって得られた効果」のトップが「社員へのセキュリティ意識の浸透と実践」が上げられている事と併せて考えても，ISMS 適合性評価制度の効果として考えられる．

4.2 企業の PDCA サイクルの現状

図 3 から，ISMS 影響下にある企業であっても情報セキュリティ対策の PDCA サイクルにおける実施率に濃淡があることがわかる．これは，情報セキュリティ対策を PDCA サイクルで実施することが出来ていない可能性を示している．P(Plan) で実施する内容として，インシデントをどの程度の発生頻度に押さえるのかという「インシデント発生頻度目標の設定 (Q10)」の実施率は 59%となっている．そして，D(Do) にあたる「インシデント発生検知手順策定 (Q22)」の実施率は 84%であり，C(Check) にあたる「実インシデント発生頻度把握 (Q23)」の実施率は 49% 「インシデント発生目標の達成確認 (Q24)」の実施率は 27%となっている．この結果から計画時にインシデント発生頻度目標の設定がされていないことは，実態を把握してもその善し悪しの判断をする指標を持っていないことであり，結果として実態把握のモチベーションを下げ，実態の把握が行われていないことが推測できる．さらに，目標も設定されておらず，実態の把握もされていないため，導入された対策について有効性も測定できてないといえる．

Vol.2009-CSEC-46 No.39
2009/7/3

しかし，そのように目標の設定も実態の測定も有効性の測定も実施されていない状況であっても，A(Action) の際の「インシデント発生情報の適用 (Q33)」の実施率は 41%となっている．これは，発生したインシデントが次のアクションの契機となることを示している．

以上をまとめると，企業の情報セキュリティ対策において，情報セキュリティ対策目標値 (P) も実際の値も測定 (D) も行われず，このため対策の有効性測定 (C) が行われずに，発生したインシデントを契機とした対策の実施が行われる (A) という，本来 ISMS が求めている姿とはかけ離れた現実が推測できる．

4.3 インシデントと脅威それぞれの内容と発生頻度認識率

4.2 節において，企業の情報セキュリティ対策活動の PDCA における P(Plan) において，インシデントの内容の把握については，高い実施率を示したが,「インシデントの発生頻度目標の設定 (Q10)」については低い実施率となっていた．発生頻度目標が定められない原因として，管理者はインシデントの内容については認識していても，頻度については把握していないという可能性が考えられる．

そこで，ISMS 影響下にある管理者の，起こりうるインシデントの内容とその発生頻度，起こりうる脅威の内容とその発生頻度それぞれの特定実施率を，図 5 に示す．結果として，脅威についてもインシデントと同様の傾向が見られた．内容の特定実施率は高いが，発生頻度特定の実施率は低い．つまり，インシデントにおいても脅威においても,「何が起きるかは分かるが，どれくらい起きるかは分からない」という状況で情報セキュリティ対策を実施していることが分かる．これは，ISMS 影響下にない回答者でも同様である (図 6)．

インシデントや脅威の発生頻度を特定する手法として，統計的な発生頻度情報の利用が考えられる．インシデントの発生頻度については，企業による事故の報告であるため，全ての情報を手に入れる事が難しく，統計的な情報を得ることが困難であると考えられる．しかし，脅威の発生頻度に関しては，IDS や Firewall のログ，またはインターネット上の定点観測 (ISDAS[4],@police[5]) などの統計情報を活用し，実施する事が可能な脅威も存在する．そこで，この統計情報の利用についての実施率を図 7 に示す．

ISMS 影響下における管理者の統計情報の利用の実施率は 18%であり，統計情報の利用について，殆ど実施されていない状況が明らかである．この結果からも，企業における情報セキュリティ管理者のインシデントや脅威における発生頻度把握の実施に課題があることが確認できた．

4.4 利害関係者

3.2 節にて示したとおり，ISMS 影響下にある管理者の中で，企業の情報セキュリティ対策

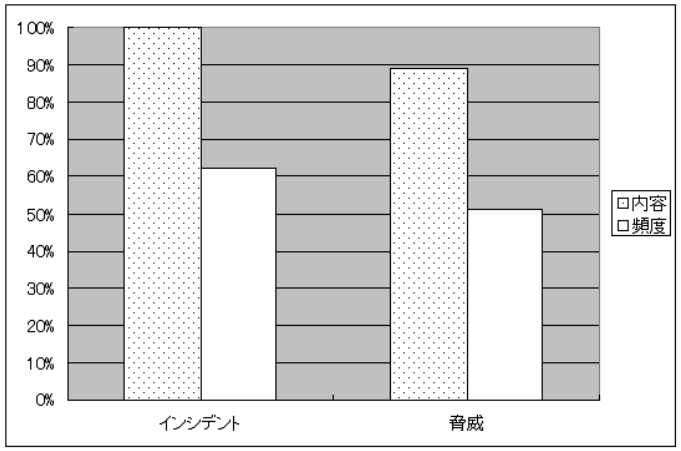

図 5 内容と頻度の特定実施率 (ISMS 影響下にある管理者．n=37)

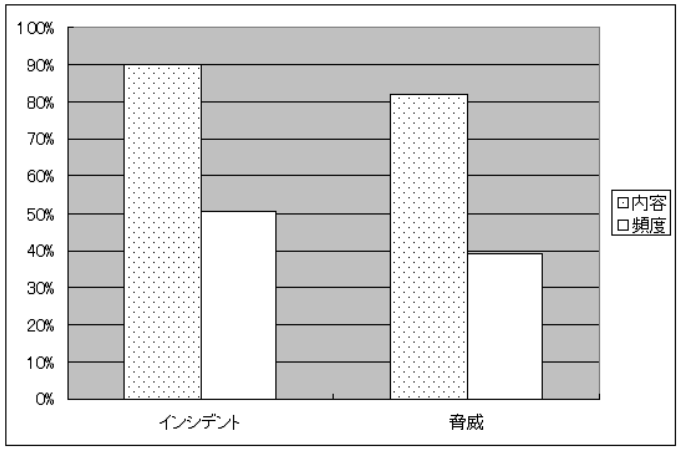

図 6 内容と頻度の特定実施率 (非 ISMS 影響下にある管理者．n=320)

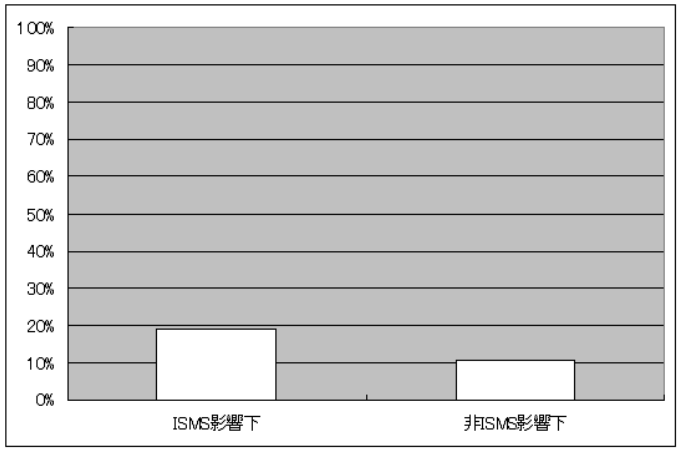

図 7 統計情報の利用実施率 (ISMS 影響下 n=37，非 ISMS 影響下 n=320))

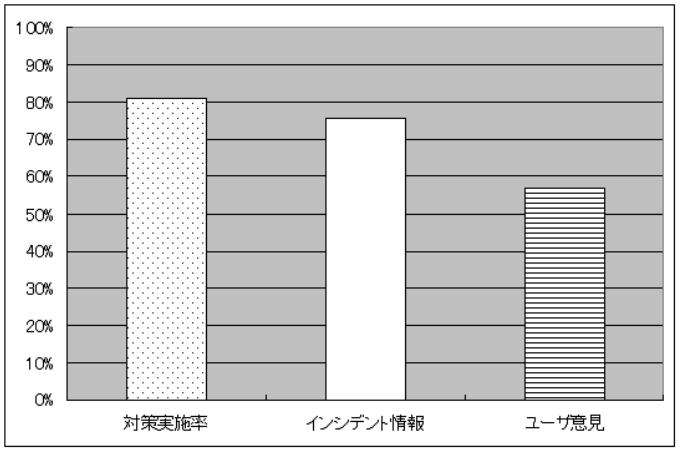

図 8 情報収集方法の見直し実施率 (ISMS 影響下における管理者．n=37)

にユーザ情報の適用を行っている管理者は 43% であり，インシデント情報の適用も 41%であった．この結果から，インシデント情報もユーザの意見も企業の情報セキュリティに対して，それほど高くはないものの同程度の影響を与えているということが考えられる．

しかし，これに関して実際には取りあげる情報に差がある可能性を示す調査結果を示す．図 8 は，企業における情報セキュリティの実施にあたって，収集することが考えられる 3 つの情報（情報セキュリティ対策の実施率，インシデント情報，ユーザの意見）それぞれの情報収集方法の見直し実施率である．

「対策の実施率」の収集方法の見直し実施率については 81%の実施率となり,「インシデント情報」の収集方法見直しについては 76%がの実施率,「ユーザ意見」の収集方法見直しは 57%の実施率であった．これらから考えられる事として，同様に「活用する」と回答されているインシデント情報とユーザ意見であるが，その収集方法についての見直しの実施率には差異があり，情報の種類によって情報収集への取り組みに違いが有ることが分かる．この結果から，情報によって得られる情報の精度や情報が届くまでの速度の違い等を産む可能性を推測することが出来る．

この「ユーザの意見」については，JIS Q 27001:2006 において重要な情報である．図 2 に，JIS Q 27001:2006 における利害関係者の位置づけを示す．JIS Q 27001:2006 においては，各所に「利害関係者」という言葉が登場する．本調査で着目した PDCA サイクルを示す *0.2.2* 項において，利害関係者からの情報セキュリティの要求事項及び期待を PDCA サイクルへのインプットとし，アウトプットとして運営管理された情報セキュリティが利害関係者へと記述されている．

しかしこの結果は，PDCA サイクルの実施が企業において行われていないのと同様に，利害関係者 1 人である「ユーザ」の意見が取り入れられていない可能性を示している．

また PDCA サイクル内でも，C(Check) では利害関係者からのフィードバックを入れる事 (*4.2.3 b)*) や，A(Action) の際には利害関係者への改善策を伝えることと，合意を得ることと記述されており (*4.2.4 c)*)，インシデント情報と並んで重要な情報である．

しかし，ISMS 影響下にある管理者にとっても，利用者からの声はそれほど重要視されていない事が推測できる．また，同様の内容が，ISMS の影響下にない回答でも見られている．図 9 に結果を示す．

5. ま と め

本調査では，企業の情報セキュリティ対策の実態調査を Web アンケート形式で実施した．質問項目を ISMS 適合性評価制度で使用される JIS Q 27001:2006 と対応付け PDCA サイクルに分類し，それらを元に企業の PDCA サイクルの現状について分析を行った．

その結果として，企業の PDCA サイクルにおける課題点が明らかになった．セキュリティ

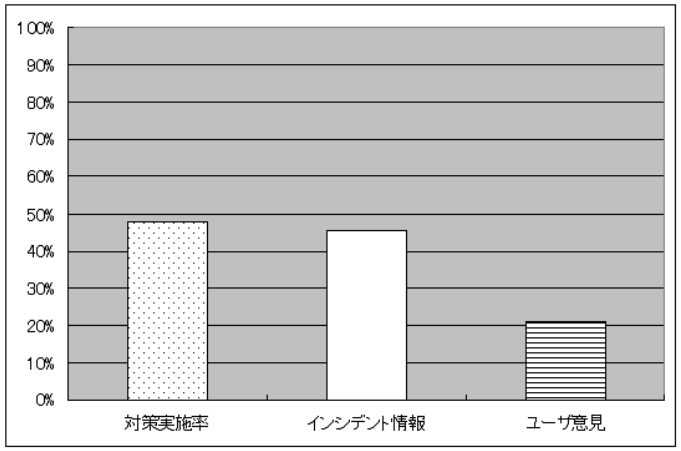

図 9 情報収集方法の見直し実施率 (非 ISMS 影響下における管理者．n=320)

対策の実施における PDCA サイクルにおいて，プロセス毎あるいはプロセスの中でも情報毎に実施率に高低が見られた．これにより，企業における情報セキュリティの PDCA サイクルに断絶が見られることが推測できた．

特に，インシデントや脅威の発生頻度に関係した,「インシデント発生頻度目標目標の設定 (Q10)」(Plan),「実インシデント発生頻度 (Q23)」(Check),「インシデント発生目標の達成確認 (Q24)」(Check)，それぞれにおいて低い実施率が確認できた．この結果から，実施された情報セキュリティ対策が，達成目標の設定もされず，実態の把握もされず，従って有効性の測定もされていないという情報セキュリティ対策における PDCA サイクルの断絶が推測された．

また，ユーザ意見の情報セキュリティへの適用について，低い実施率が確認できた．これは，JIS Q 27001:2006 にて記述されている，利害関係者から PDCA サイクルへのインプット等が行われていない可能性があり，企業の情報セキュリティにおける PDCA サイクルと，利害関係者の関係について課題があることが推測された．

6. 今後の課題

課題の 1 点目として，より広い範囲の調査の実施である．本調査では標本数が少なく，ISMS 影響下の管理者という回答者群の傾向のみしか扱えなかった．今後の調査では標本数を増やし，PDCA サイクルの断絶の原因等ついて，より詳細な分析を行う予定である．

課題の 2 点目として，PDCA サイクルにおける利害関係者に関する調査の実施である．本調査では利害関係者である情報セキュリティ対策のユーザについて，ユーザ意見がどれだけ対策に影響を与えているかを調査した．結果としてはユーザの意見は情報セキュリティ対策へあまり影響を与えていないという状況が推測された．今後は利害関係者のスコープを広げ，ユーザだけでなく一般的な利害関係者の意見と情報セキュリティ対策の関係について，調査をしていく必要があると考えている．

参 考 文 献

1) JIS Q 27001:2006　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
2) 財団法人　日本情報処理開発協会適合性評価制度の概要,2007 年 12 月
3) 財団法人ニューメディア開発協会,「ISMS の維持管理における実態調査」，2009 年 3 月
4) JPCERT/CC, インターネット定点観測システム ISDAS,http://www.jpcert.or.jp/isdas/
5) 警察庁，警察庁セキュリティポータルサイト@police,http://www.cyberpolice.go.jp/detect/observation.html
6) 財団法人　日本情報処理開発協会　情報マネジメント推進センター,ISMS 適合性評価制度に関するアンケート調査報告書