

平成 13 年度 セキュリティ対策研究開発等事業

情報セキュリティの実態調査 2001
調査報告書

情報処理振興事業協会

セキュリティセンター



目次

調査報告書サマリー	3
第1章 調査目的	5
第2章 調査概要	6
1. 調査体制	6
2. 調査対象	6
3. 調査期間	6
4. 配布・回収方法	7
第3章 分析概要	8
1. 調査票の作成手順	8
2. 分析属性の設定	14
3. ベンチマーク軸の設定	17
第4章 調査結果	19
1. 回収状況	19
2. 回答者分布	19
2.1. 回答企業基本属性	20
2.1.1. 従業員数	20
2.1.2. 拠点数	20
2.1.3. 年間売上	21
2.1.4. 主要業種	21
2.2. 回答者情報	22
2.2.1. 所属部門	22
2.2.2. 役職	22
2.2.3. 経験業務	23
2.3. 回答企業システム構成	24
2.3.1. 保有コンピュータ台数	24
2.3.2. インターネットへの接続方法	24
2.3.3. LANの有無	25
第5章 分析結果	26
1. 全体傾向	26
2. 情報セキュリティマネジメントの実態把握	28
2.1. 情報セキュリティポリシーの整備状況	28
2.2. 情報セキュリティ管理体制の整備状況	32
2.3. 情報セキュリティ教育体制の整備状況	38

2.4.	アクセス制御の実施状況.....	41
2.5.	モニタリングの実施状況.....	43
2.6.	システム導入及び構成変更に関する安全性の確保状況.....	45
2.7.	アカウントビリティの確保状況.....	50
2.8.	情報セキュリティ管理のためのリソースの確保状況.....	52
2.9.	技術的な情報セキュリティの確保状況.....	55
3.	情報セキュリティ対策（インシデント対策）の問題点把握.....	56
3.1.	情報セキュリティ問題による被害状況.....	56
3.2.	情報セキュリティ問題の原因.....	57
3.3.	情報セキュリティ問題に関する対応体制の整備状況.....	58
3.4.	情報セキュリティ問題に関する対応技術の習熟度.....	61
3.5.	情報セキュリティ問題発生時のアカウントビリティの確保状況.....	64
4.	情報セキュリティマネジメント 対策の改善方法の検討.....	69
4.1.	今後の情報セキュリティ対策の整備計画（自社整備、アウトソーシング）...	69
4.2.	公共団体への期待.....	70

調査報告書サマリー

情報セキュリティの実態調査 2001 (以下「本調査」という)は、日本国内の民間企業における情報セキュリティの実態を明らかにすることを目的とした調査プロジェクトである¹。本プロジェクトでは、情報セキュリティに関連した実態を包括的に把握するために、以下の3つの調査目的を設定した。

情報セキュリティマネジメントの実態把握

情報セキュリティ問題への対策(インシデント対策)の問題点把握

情報セキュリティマネジメント・情報セキュリティ対策の改善方法の検討

本調査目的は、情報技術または組織の一方に偏ることなく、情報セキュリティで必要とされる技術、運用、組織管理等についての包括的な調査を実施した。

本調査では、2001年12月に日本国内の民間企業5,000社を対象に調査票を送付した。回答企業数は550社、回収率は11%だった。

本調査から得られたデータは、企業の規模や業種による情報セキュリティの管理体制の差異が把握できるように集計した。また、情報セキュリティに対応するための組織の体制整備と情報セキュリティ関連の技術導入状況の特徴が把握できるように集計した。

調査結果の中で特筆すべき点として、6点挙げることとする。

(1) 回答者分布

本プロジェクトでは、小規模企業から大企業まで企業規模に偏りなく、調査票を送付した。しかし、回答企業の約84%が売上高5億以上の企業であった。つまり小規模企業と比較して、大企業の回収率が高かったといえる。このことから、現時点の日本の小規模企業では情報セキュリティに対する意識や興味が低いのではないかと推察できる。

(2) 企業規模別傾向

本プロジェクトでは、回答結果を点数化するベンチマークを実施した。ベンチマーク集計の結果、従業員数が多い企業ほど情報セキュリティマネジメントのベンチマークの平均点数が高かった。また、従業員数が多い企業ほど情報セキュリティ関連技術の導入種類が多かった。情報セキュリティに対するマネジメント、技術の両面で従業員数の多い企業ほど対策が進んでいることが判明した。また、売上高が高いほど情報セキュリティ管理者を設置している企業の割合が高かった。情報セキュリティ管理における組織マネジメントという観点では、企業規模による差異が顕著であった。

(3) 業種別傾向

¹本調査は、調査主体である情報処理振興事業協会セキュリティセンター(PA/ISEC)が、KPMG ビジネスアシュアランス株式会社に委託して実施した。

ベンチマーク結果の業種別平均点は、情報・通信、金融、医療・製薬、エネルギー業界の順に高得点であった。これらの4業界でベンチマークの平均点が高かった原因としては、情報セキュリティポリシーの導入、情報セキュリティ管理部門の設置、入退室管理、システム監査・ペネトレーションテストの実施が進んでいること等が挙げられる。

(4) 情報セキュリティマネジメントの実態

情報セキュリティに関連した規定をもつ企業は約60%であった。しかし、規定内容は情報システム機器の管理やコンピュータウイルス対策が中心であり、情報セキュリティ管理における責任体制の明確化を定めている企業は少なかった。情報セキュリティを管理するための「専門部門がある」と回答した企業は全体の6%であった。専門部門があると回答した企業のうち約40%の企業で、情報セキュリティの管理部門は情報システム部門に所属していた。情報セキュリティ管理を担当する部署や委員会に配属する人材に求めるスキルや経験としては、「情報技術関連」が最も多く、部門横断的なプロジェクトマネジメント能力を求める回答は少なかった。

情報セキュリティマネジメントを実践するためには、社内の情報資産を保護し有効に活用するために、部門横断的に業務を推進することのできる人材が情報セキュリティ管理者を務めることが望ましい。しかし、現状では情報セキュリティ管理者は情報システム部の情報技術スキルを有する部課長クラスの人材が任命され、担当しているという回答が最も多かった。

(5) 情報セキュリティ問題への対策（インシデント対策）の実態

情報セキュリティ問題への対策を整備するためには、情報セキュリティに関連して発生している問題を記録し、現状を把握することが大切である。しかし、情報セキュリティ問題の発生状況を「記録していない」という企業が30.7%あった。また、情報セキュリティ問題が発生した場合「担当者の裁量」により対応すると回答した企業が最も多く、業務継続計画や情報セキュリティ対策手順等を整備し包括的に対処を進める企業は少なかった。

一方、約70%の企業で情報セキュリティ問題が発生した場合に「社内啓発のため」に問題の発生を社内告知しており、情報セキュリティ問題を啓発・教育の機会と捉えている姿勢が推察できた。

(6) 公共団体に対する要望

情報セキュリティ対策に関連して公共団体に希望する対策として、業種や企業規模に関わらず全般的に「安価なセキュリティ教育」や「セキュリティ教育コンテンツ」の提供及び「セキュリティ啓発活動」を望む声が高かった。

第1章 調査目的

本調査の目的は、日本国内の民間企業における情報セキュリティの実態を明らかにすることである。情報セキュリティの実態に関する包括的な情報を収集するために、以下の3点を調査目的として設定した。

- (1) 情報セキュリティマネジメントの実態把握
- (2) 情報セキュリティ問題への対策（インシデント対策）の問題点把握
- (3) 情報セキュリティマネジメント・情報セキュリティ対策の改善方法の検討

(1) 情報セキュリティマネジメントの実態把握

組織における情報セキュリティの管理体制や運用体制を明らかにするために設定した調査目的である。情報セキュリティを確保するためには、情報セキュリティ関連製品の導入と同時に、導入した製品の日々の管理や運用、また情報システムを利用する人材の管理体制や運用体制、教育体制も重要である。「情報セキュリティ技術」ではなく、技術を効果的に利用するための管理を「情報セキュリティマネジメント」と呼ぶ。

(2) 情報セキュリティ問題への対策（インシデント対策）の問題点把握

情報セキュリティ問題（情報セキュリティに関連する事故や事件）が発生した場合の対応体制を明らかにするために設定した調査目的である。情報セキュリティ関連の事故や事件が発生するリスクを0にすることは難しい。情報セキュリティ対策を十分に講じていると考えている企業であっても、情報セキュリティ問題が発生する可能性はある。そのため、あらゆる企業では情報セキュリティ問題が発生した場合の対応体制を整備する必要がある。本調査項目では、情報セキュリティ問題が発生した場合の、企業の対処方法や今後の対処予定についての情報を収集した。

(3) 情報セキュリティマネジメント・情報セキュリティ問題対策の改善方法の検討

情報セキュリティ管理の行為主体として自社、グループ企業、業界団体、公共団体等で実施すべきであると考えている施策や情報セキュリティ対策を実施する場合の問題点を明らかにするために設定した調査目的である。情報セキュリティ管理は、技術導入や組織マネジメントだけではなく、社外との関係改善や業界全体での方針の統一等が必要な場合があり、自社だけで実行することは難しいといえる。情報セキュリティ管理を継続的な活動として捉え、自社だけではなく公共団体や業界団体が協力して情報セキュリティの向上を目指すためには、どのような施策が必要であるのか、また望まれているのかといった意識についての情報を収集した。

第2章 調査概要

本章では、本調査の調査概要として、調査体制、調査対象、調査期間、配布・回収方法を記載する。

1. 調査体制

本調査の調査主体は「情報処理振興事業協会セキュリティセンター」である。「KPMG ビジネスアシュアランス株式会社」は「情報処理振興事業協会セキュリティセンター」より委託を受け本調査を実施した。

表 2-1 調査体制

主体	情報処理振興事業協会セキュリティセンター (PA/ISEC) ²
実施	KPMG ビジネスアシュアランス株式会社 ³

2. 調査対象

本調査の調査対象は日本国内の民間企業である。また、回答者としては当該企業で情報セキュリティに関する責任を有する人材を想定した。欧米であればCISO⁴という言葉も一般化しつつあり CISO 宛に調査票を送付することも可能であろう。しかし、日本国内では情報セキュリティに関する責任者を正式に任命している企業は少ない。そのため、調査票を送付する封筒の宛先は「情報システム部門長」とし、挨拶状の中に情報セキュリティを担当する方に調査票を転送するよう依頼文を掲載するという方法を採用した。

表 2-2 調査対象

調査対象	日本国内の民間企業
想定回答者	情報セキュリティ管理者
宛先名	情報システム部門長

3. 調査期間

調査票の発送及び回収締め切りは下記の日程で実施した。

表 2-3 調査期間

発送開始日	回収有効消印日付
2001年12月7日	2001年12月31日

調査票発送時に同封した挨拶状には 2001 年 12 月 20 日を最終返送期限と記載した。しかし、期限延長を希望する問合せが多かったため返送期限を延長した。

² URL: <http://www.ipa.go.jp/security/>

³ URL: <http://www.kpmg.or.jp/>

⁴ Chief Information Security Officer のこと。情報セキュリティ最高責任者、情報セキュリティ担当役員。

4. 配布・回収方法

本調査は普通郵便による送付、回収により実施した。回答者からは回答用紙のみ返送を依頼した⁵。「付録篇」に調査票・回答用紙を添付している。詳細は「付録篇」を参照のこと。

表 2-4 送付 返信内容一覧

送付封筒同封書類一覧	挨拶状 (調査依頼文)
	IPA/ISEC 事業概要案内
	調査票
	回答用紙
	返信用封筒
ベンチマーク (例)	
返信用封筒同封書類一覧	回答用紙

また、本調査では希望のあった回答者に対して、回答結果の一部を利用したベンチマーク結果を電子メールに添付の上送付した。「付録篇」にベンチマーク例を添付している。ベンチマークの形式等の詳細は「付録篇」を参照のこと。

⁵ 回収枚数 550 枚中 5 枚は回答者が調査票に直接回答を記入したものだ。調査票には電子メールアドレスの記入欄がなく、欄外等にも電子メールアドレスが未記載であったためベンチマーク結果を送付できなかった企業が 2 社あった。

第3章 分析概要

本章では、調査票の作成手順、分析属性の各項目の設定理由の概略を記載する。調査票は、調査目的に対する調査項目、質問の意図を設定した上で質問及び選択肢を作成した。分析属性は、各設問とのクロス集計を実施するための設問項目である。調査票の属性設問（設問番号：A-1～C-3）以外に、調査目的を満足させるために必要な属性を追加した。ベンチマークは、回答企業が情報セキュリティ対策を実施するにあたって特に有効であると考えられる設問内容の一部を選択し、その設問に対する回答結果を点数化したものである。各評価対象の点数を5本の軸にマッピングして表示すると同時に他社との比較のために業界平均、全体平均を合わせて表示した。

1. 調査票の作成手順

本節では、調査票の作成の設定手順を説明する。第一に、調査目的を複数の調査項目に分類する。第二に、各調査項目に分類すべきであると考えた理由を質問の意図として記載する。第三に、質問の意図を満足させるために必要な設問と回答の選択肢を列挙する。

個々の質問を調査目的から直接設定すると、網羅性を欠く可能性が高い。調査目的を満足させる質問を設定するためには、質問内容を類型化した中項目が必要である。そのため、本調査では中項目として調査項目を設定し、調査データを分析する際の指針を明らかにするために質問の意図を記載した上で質問を設定した。

調査項目の設定では、網羅性を確保するために、BS7799 及び ISO/IEC TR13335 (GMITS) 等の情報セキュリティマネジメントに関する国際規格を参照した。また、KPMG グループがシステム監査の際に使用する ITRMB⁶ の調査項目を参照し、多面的な視点で設定した。

上述の方法で調査項目を設定した結果、情報セキュリティマネジメントの実態把握では9つの調査項目、情報セキュリティ問題への対策（インシデント対策）の問題点把握では5つの調査項目、情報セキュリティマネジメント・情報セキュリティ対策の改善方法の検討では2つの調査項目を設定した。

表3-1は調査目的と調査項目の対応関係を表している。表3-2～表3-4は各調査項目と質問の意図及び調査票の設問番号の関係を表している。

⁶ ITRMB (IT Risk Management Benchmarking) は、企業における情報システム関連リスクおよびコントロールの状況を、同業他社等とのベンチマークを含め、総合的に評価することができる KPMG のシステム監査用メソッドロジー（方法論）である。特に、組織のマネジメント体制整備状況に関する設問が豊富である。

表 3-1 調査目的 調査項目対応表

調査目的	調査項目
(1) 情報セキュリティマネジメントの実態把握	情報セキュリティポリシーの整備状況
	情報セキュリティ管理体制の整備状況
	情報セキュリティ教育体制の整備状況
	アクセス制御の実施状況
	モニタリングの実施状況
	システム導入及び構成変更に関する安全性の確保状況
	説明責任(アカウントビリティ)の確保状況
	情報セキュリティ管理のためのリソースの確保状況
	技術的な情報セキュリティの確保状況
(2) 情報セキュリティ問題への対策(インシデント対策)の問題点把握	情報セキュリティ問題による被害状況
	情報セキュリティ問題の原因
	情報セキュリティ問題に関する対応体制の整備状況
	情報セキュリティ問題に関する対応技術の習熟度
	情報セキュリティ問題発生時の説明責任(アカウントビリティ)の確保状況
(3) 情報セキュリティマネジメント・情報セキュリティ対策の改善方法の検討	今後の情報セキュリティ対策の整備計画(自社整備、アウトソーシング)
	公共団体への期待

(1)情報セキュリティマネジメントの実態把握

第1の調査目的である情報セキュリティマネジメントの実態把握に対して設定した9つの調査項目毎に、質問の意図及び対応する設問番号を記載する。

表3-2 情報セキュリティマネジメントの実態把握の設問構成

調査項目	質問の意図	設問番号
	情報セキュリティポリシーの整備状況	
	情報セキュリティポリシーの導入状況の確認	1-1、1-3、1-5
	情報セキュリティポリシーの規定内容の確認	1-2
	情報セキュリティポリシーのメンテナンス状況の確認	1-4
情報セキュリティ管理体制の整備状況		
	情報セキュリティ専門部門の設置状況、配置されているメンバーのスキルの確認	1-6、1-7、1-8
	全社責任者(CISOの有無、職位)の任命状況、スキル・教育の確認	1-9、1-10、1-11、1-12
	役割・責任分担体制、命令・報告系統の確認及び組織内における周知度合いの確認	1-13、1-14、1-15
	業者管理・外部委託管理上のリスク認識度合い、機密保持契約や与信体制の整備状況の確認	1-16、1-17
	事業継続、普及体制の整備状況の確認及び代替手段の確保状況、データバックアップ、遠隔地保管等の確認	1-18、1-19、1-20、1-21、1-22
情報セキュリティ教育体制の整備状況		
	セキュリティポリシー上の情報セキュリティに関する教育の規定有無、実施有無、実施レベルの確認	1-23、1-24、1-25、1-26
アクセス制御の実施状況		
	情報セキュリティ確保のための物理アクセス制御の現状確認	1-27、1-28、1-29、1-36
モニタリングの実施状況		
	アクセス制御・監視・パスワード管理の実施状況の確認	1-30、1-31、1-32

システム導入及び構成変更に関する安全性の確保状況		
	構成変更の手順(個人の端末含)の確認	1-33、1-34、 1-35
	アプリケーションライセンス管理(個人の端末含)の確認	1-37
	標準化ルールの有無と、その定着度の確認	1-38
説明責任(アカウンタビリティ)の確保状況		
	法令・ガイドライン・行政指導の確認担当者の設置、定期的な確認及び従業員への周知、遵守状況の確認	1-39、1-40
	情報セキュリティや技術についての準拠規定の有無と、準拠状況の確認	1-41
	システム監査、業務監査の実施状況、監査改善報告への対処方法の確認	1-42、1-43、 1-44
情報セキュリティ管理のためのリソースの確保状況		
	予算、人員確保(IT、情報セキュリティ、インシデント時の予算)の現状の確認	1-45、1-46
技術的な情報セキュリティの確保状況		
	情報セキュリティを確保するために全社的に導入している技術的対策の確認	1-47

(2)情報セキュリティ問題への対策(インシデント対策)の問題点把握

第2の調査目的である情報セキュリティ問題への対策(インシデント対策)の問題点把握に対して設定した5つの調査項目毎に、質問の意図及び対応する設問番号を記載する。

表 3-3 情報セキュリティ対策の問題点把握の設問構成

調査項目		設問番号
質問の意図		
情報セキュリティ問題による被害状況		
	発生したインシデントの種類とその対応に要した人日等の被害状況の確認	2-2
情報セキュリティ問題の原因		
	インシデントが発生した原因の確認	2-1
情報セキュリティ問題に関する対応体制の整備状況		
	インシデントが発生した場合の体制整備状況の確認(組織内の連絡体制、顧客被害の把握方法等)	2-3、2-4、 2-5
	インシデント対応時の有効性の確認(復旧に要した時間、顧客被害額、防災訓練との違い、外部コンサルの利用等)	2-6
情報セキュリティ問題に関する対応技術の習熟度		
	インシデントハンドリングを行うことのできる人材・手段の有無の確認	2-7
情報セキュリティ問題発生時の説明責任(アカウントビリティ)の確保状況		
	広報体制の整備状況の確認	2-8
	広報内容の切り分けの確認	2-9
	外部リソースの利用によるアカウントビリティの確保体制の確認	2-10

(3)情報セキュリティマネジメント 情報セキュリティ問題対策の改善方法の検討

第3の調査目的である情報セキュリティマネジメント 情報セキュリティ対策の改善方法の検討に対して設定した2つの調査項目毎に、質問の意図及び対応する設問番号を記載する。

表 3-4 今後の改善方法の検討の設問構成

調査項目		設問番号
	質問の意図	
今後の情報セキュリティ管理の整備計画 (自社整備、アウトソーシング)		
	今後実施すべき、実施が望ましいと考えているセキュリティ改善施策の確認	3-1
	自社で対応が可能だと考えているセキュリティ改善施策の確認	3-2、3-3
	今後、業界、グループとして対応を希望するセキュリティ改善施策の確認	3-4
	業界、グループとしての対応を阻害する要因として把握しているものの確認	3-5
	外部委託で対応を希望するセキュリティ改善施策の確認	3-6
	外部委託の阻害要因として把握しているものの確認	3-7
公共団体への期待		
	自社で対応が難しい対策のうち、公共団体が実施すべきだと考える施策の確認	3-8、3-9、3-10

2. 分析属性の設定

本調査から得られたデータは、今後 IPA/ISEC が情報セキュリティに関する基礎データとして利用する。また、公開された分析結果は各企業が自社の情報セキュリティの向上を目指す際の参考資料として利用することも考えられる。そこで、企業の規模や業種による情報セキュリティの管理体制の差異が把握できるように分析属性を設定した。また、情報セキュリティに対応するための組織の体制整備と情報セキュリティ関連の技術導入状況の特徴の把握という観点からの分析属性も設定した。

分析属性として設定した設問項目は、表 3-5～表 3-9 の通りである。分析属性は、全設問とクロス集計し、「全数カウント結果」として「第 3 篇 集計結果篇」の第 2 章に記載した。

(1)回答企業基本属性

回答企業基本属性では、下記の 4 項目を設定した。

表 3-5 回答企業基本属性一覧

No.	設問番号	タイトル	選択肢	選択肢数
	A-1	従業員数	a～g*、未記入	8
	A-2	拠点数	a～e*、未記入	6
	A-3	売上	a～d*、未記入	5
	A-4	業種	a～j、未記入	11

* 選択肢の詳細は「付録篇」に添付の調査票原本を参照。

(2)回答者情報

回答者情報では、下記の 3 項目を設定した。

表 3-6 回答者情報別属性一覧

No.	設問番号	タイトル	選択肢	選択肢数
	B-1	職制	情報システム (e, f)*、情報システム以外 (a, b, c, d, g, h)*、未記入	3
	B-2	職位	経営 役員 (a, b)*、中間管理職 (c, d)*、一般社員 (e, f)*、未記入	4
	B-3	情報システム部門経験	経験有り (e, f 有)*、経験無し (e, f 無)*、未記入	3

* 選択肢の詳細は「付録篇」に添付の調査票原本を参照。

(3) 回答企業システム構成

回答企業システム構成では、下記の3項目を設定した。

表 3-7 回答企業システム構成別属性一覧

No.	設問番号	タイトル	選択肢	選択肢数
	C-1	PC 台数	a~e*、未記入	6
	C-2	帯域	なし(a)*、ダイヤルアップ(b)、専用線以外(c、d)*、専用線(e、f、g)*、その他(h、未記入)*	5
	C-3	LAN 有無	ある(a)*、なし(b)*、未記入	3

*選択肢の詳細は「付録篇」に添付の調査票原本を参照。

(4) その他

本調査では情報セキュリティポリシーの有無や、情報セキュリティ管理者・管理部門の有無等の違いによる情報セキュリティ対策の違いに関する情報を収集するために、情報セキュリティ管理において重大な影響を与えると考えられる属性を設定した。

表 3-8 回答企業システム構成別属性一覧

No.	設問番号	タイトル	選択肢	選択肢数
	1-1	セキュリティポリシー有無	あり(2~6)*、なし(1)*、その他(7、8、未記入)*	3
	1-6	管理部門有無	あり(2~5)*、なし(1)*、その他(6、7、未記入)*	3
	1-9	管理者有無	あり(2、3)*、なし(1)*、その他(4、未記入)*	3
	1-20	業務継続計画(Business Continuity Plan:BCP)有無	あり(2)*、なし(1、3、4、5、6)*、未記入	3
	1-30	サーバアクセスログ解析有無	あり(3)*、なし(2)*、その他(1、4、5、6、未記入)	3
	1-45	予算有無	あり(2~4)*、なし(1)*、その他(5、6、未記入)*	3
	1-47	導入技術	ネットワーク構成工夫有り(1、2、3、4、5、6、10有)*、ネットワーク構成工夫無し(1、2、3、4、5、6、10無)*、ウイルス対策有り(7、9、11有)*、ウイルス対策無し(7、9、11無)*	4
	表 3-9 ベンチマーク対象設問一覧参照	ベンチマーク点数	高(平均点×2以上)、中(平均以上高未満)、低(平均以下)	3

*選択肢の詳細は「付録篇」に添付の調査票原本を参照。

は情報セキュリティ対策の進んだ企業と比較的遅れている企業が具体的にどのような対策の実施において差異が生じているのかを把握するために設定した分析属性である。この分析属性としては「第3章 3.ベンチマーク軸の設定」で後述するベンチマークの各企業の得点数によって3つに分割して設定した。但し、ベンチマーク対象は設問の一部であり、企業の情報セキュリティ対策の実状を正確に反映していない場合もある。そのため、この属性は参考に留め詳細を検討する場合は元データに戻る必要がある。

3. ベンチマーク軸の設定

本調査では情報セキュリティの向上にあたり、特に有益であると考えられる設問のベンチマークを行った。ベンチマーク軸の設定は、対象となる設問の選定、各設問間の情報セキュリティにおける重要度での重み付け、各設問の選択肢の点数化という手順で行った。

(1)対象設問の選定

ベンチマーク軸の設定にあたり、回答者が情報セキュリティ向上にあたり、特に有益であると考えられる5つの評価対象を選定し、対応する設問を選択した⁷。評価対象及び対象設問は表3-11のとおりである。

表3-9 ベンチマーク対象設問一覧

軸	評価対象	対象設問	調査目的との対照	調査項目との対照
A	情報セキュリティ管理体制の整備状況	1-6～1-22	情報セキュリティマネジメントの実態把握	情報セキュリティ管理体制の整備状況
B	不正アクセスの監視状況	1-30～1-32、1-35、1-39、2-5		モニタリングの実施状況
C	情報セキュリティ管理のためのリソース確保の状況	1-7、1-45～1-46		情報セキュリティ管理のためのリソースの確保状況
D	情報セキュリティ問題への対応状況	1-14～1-15、2-1、2-3～2-10	情報セキュリティ対策(インシデント対策)の問題点把握	全般
E	今後の情報セキュリティ対策の立案状況	3-2～3-5	情報セキュリティマネジメント・情報セキュリティ対策の改善方法の検討	全般

⁷本調査では、希望者に回答結果を元にした各企業の情報セキュリティ管理に関するベンチマークの集計結果を電子メールにて送付した。

(2)各設問の重み付けの設定

対象となる設問を選択後に、下記の手順で点数を設定した。

各設問の情報セキュリティ管理における重要度の検討 :各設問の重要性を比較し、重み付けをする。

情報セキュリティポリシーの有無や予算の有無といった情報セキュリティ対策上重要度の高い設問と比較的重要度の低い設問を分類し各設問における得点を決定する。この重み付けには、前出のITRMBの結果及びKPMGグループのシステム監査及び情報システム関連のアシュアランスアドバイザー業務の経験を利用した。

各選択肢に点数を付与する。

各設問の最高点は で定めた得点となる。この得点となるように、各選択肢の点数を割り振る。

各軸の総合点数が同じ数値になるように割り算をする。

第4章 調査結果

本章では、本調査の調査結果の概要及び、回答者分布を記載する。

1. 回収状況

本調査の送付枚数、回収枚数、回収率は表 4-1 のとおりである。

表 4-1 回収状況

送付枚数	5,000 枚
回収枚数	550 枚
回収率	11%

2. 回答者分布

本節では、本調査の回答企業及び、回答者の属性を記載する。本調査票では、基本的な属性として 企業情報 回答者情報 企業の情報システム構成の3点についての質問を行った。

2.1. 回答企業基本属性

本調査票で設定した基本的な属性に関する設問の中で、企業情報に関する設問はA1～A4の4問あった。図4-1～図4-4では、この4問の回答結果をグラフ化して表示した。

2.1.1. 従業員数

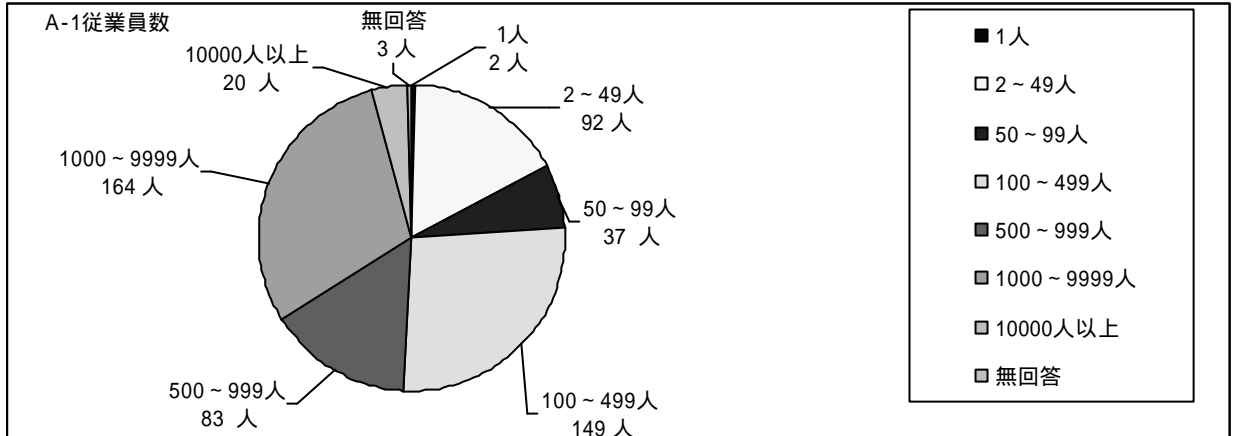


図4-1 A-1 従業員数分布

2.1.2. 拠点数

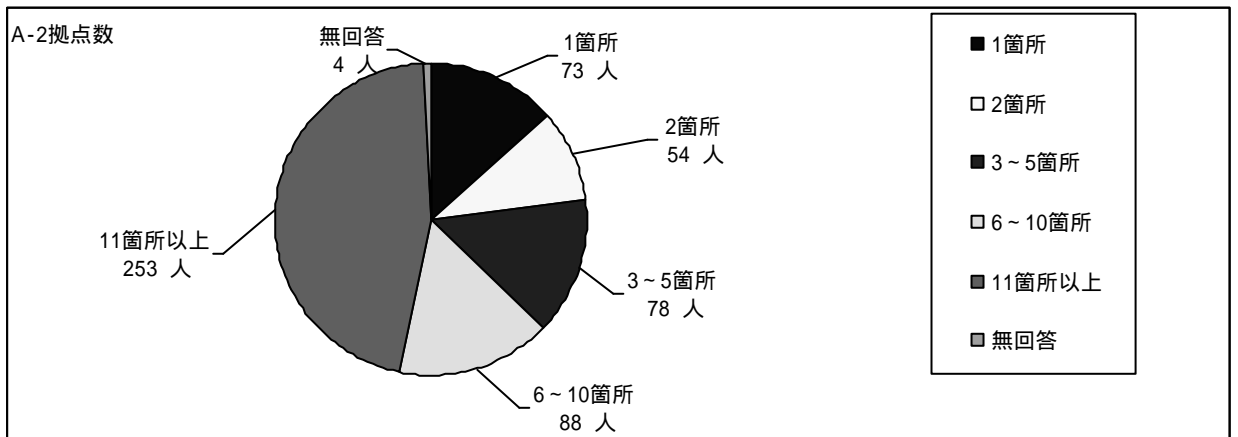


図4-2 A-2 拠点数分布

2.1.3. 年間売上

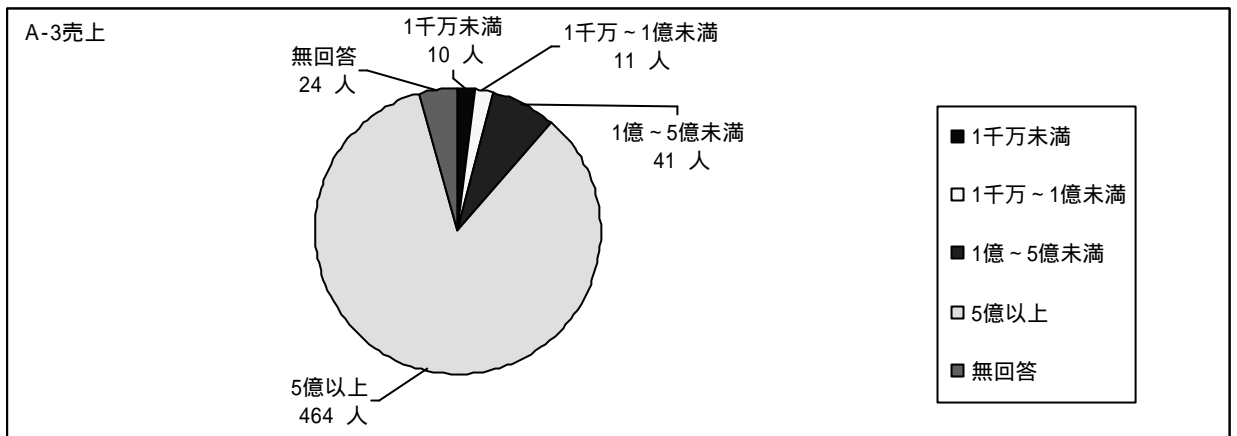


図 4-3 A-3 年間売上分布

2.1.4. 主要業種

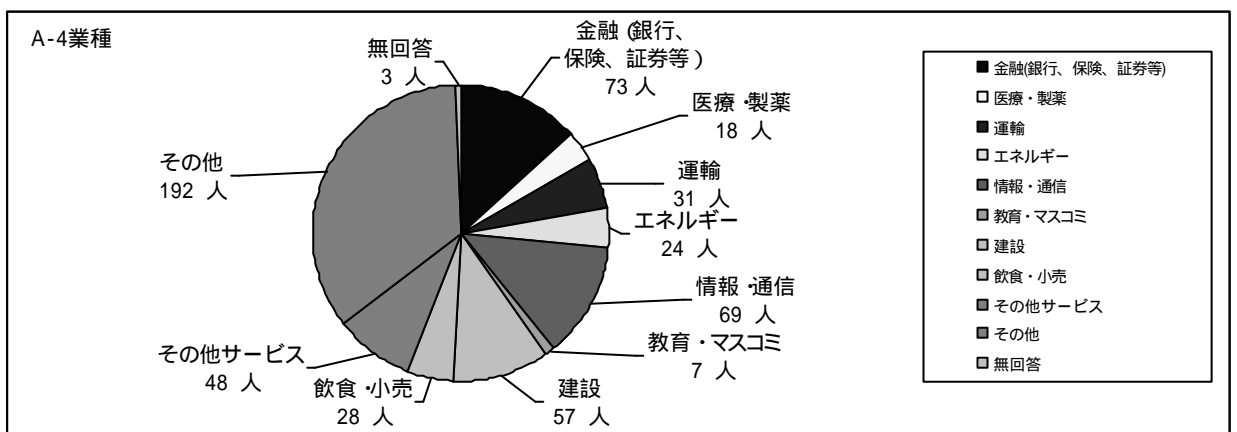


図 4-4 A-4 主要業種分布

2.2. 回答者情報

本調査票で設定した基本的な属性に関する設問の中で、回答者に関する設問は B1～B4 の4問あった。図 4-5～図 4-8 では、この4問の回答結果をグラフ化して表示した。

2.2.1. 所属部門

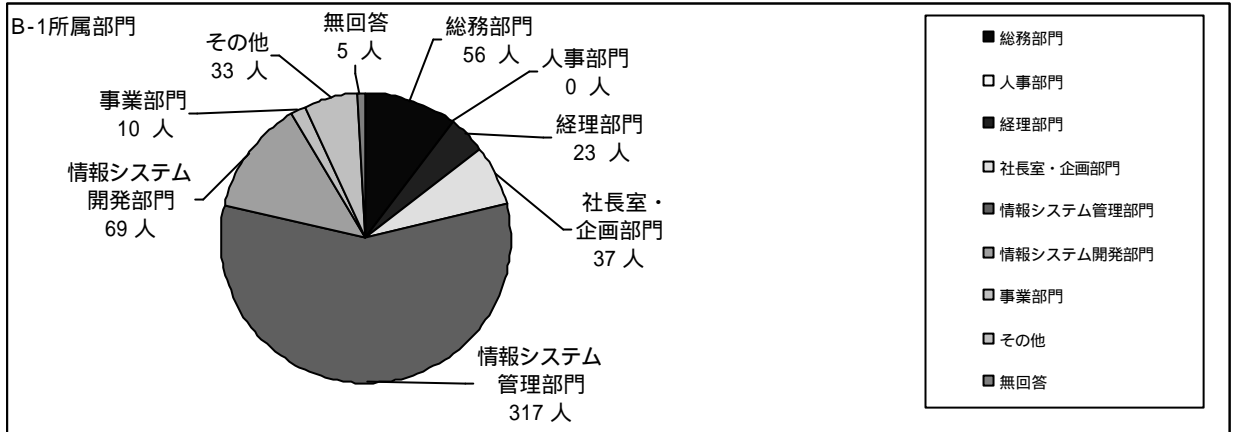


図 4-5 B-1 所属部門分布

2.2.2. 役職

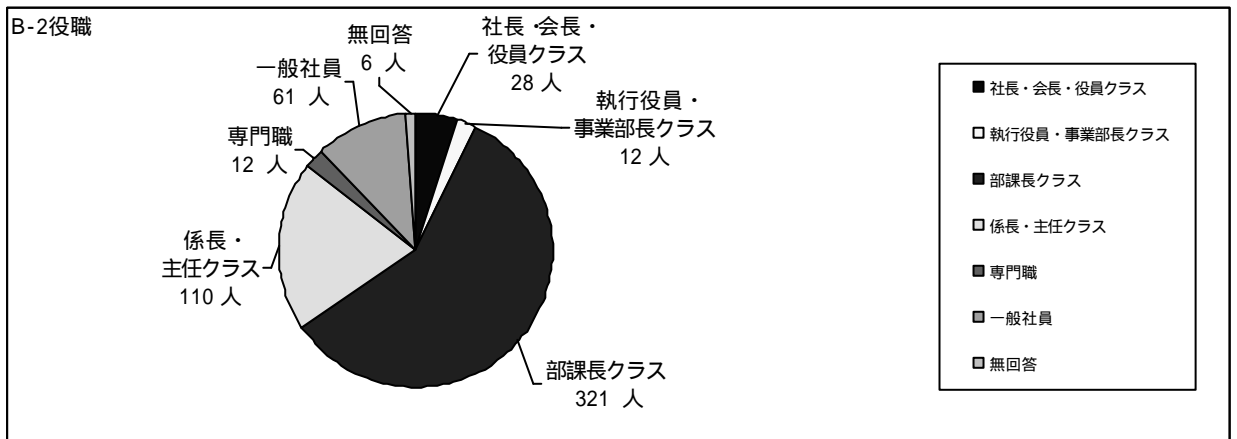


図 4-6 B-2 役職分布

2.2.3. 経験業務

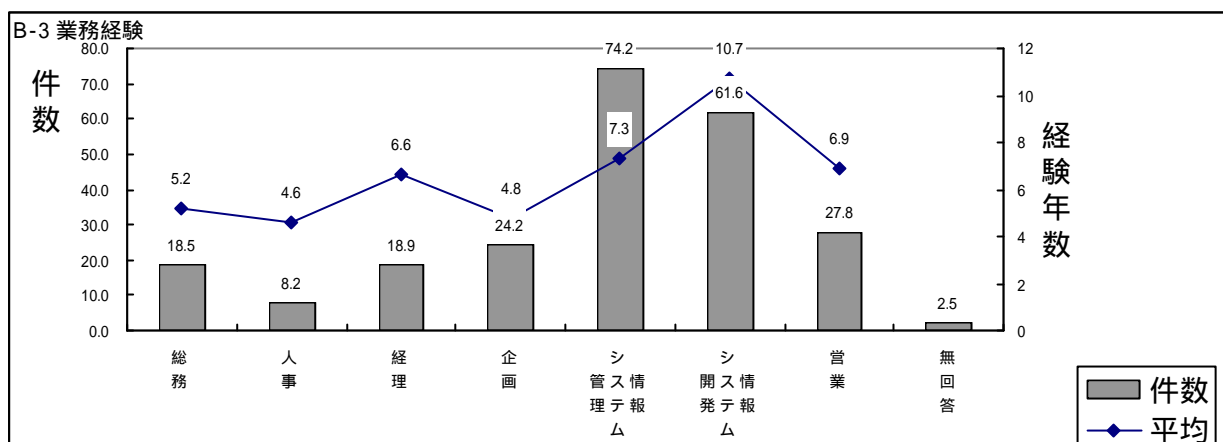


図 4-7 B-3 経験業務と経験年数の分布

2.2.4. 情報システム関連業務

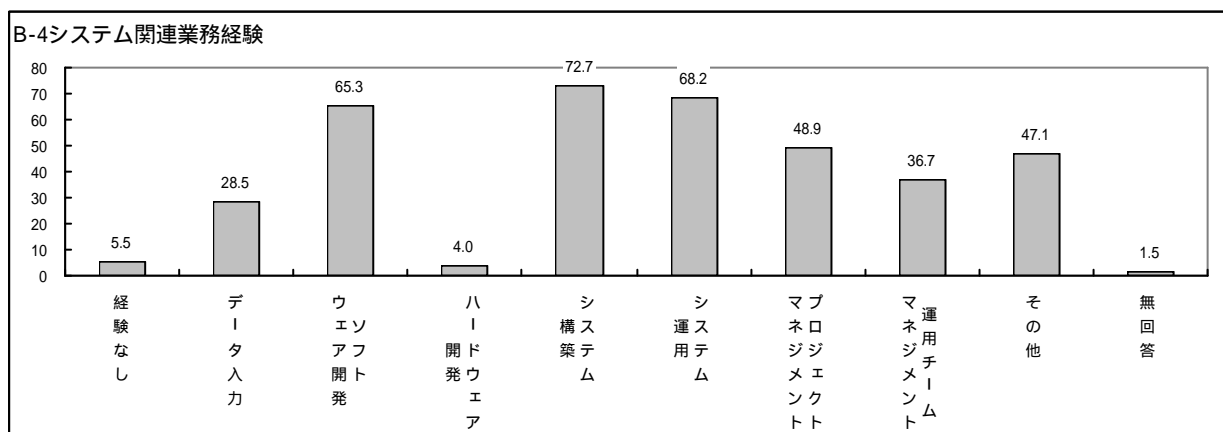


図 4-8 B-4 情報システム関連業務経験有無

2.3. 回答企業システム構成

本調査票で設定した基本的な属性に関する設問の中で、企業の情報システム構成に関する設問はC1～C3の3問あった。図4-9～図4-11では、この3問の回答結果をグラフ化して表示した。

2.3.1. 保有コンピュータ台数

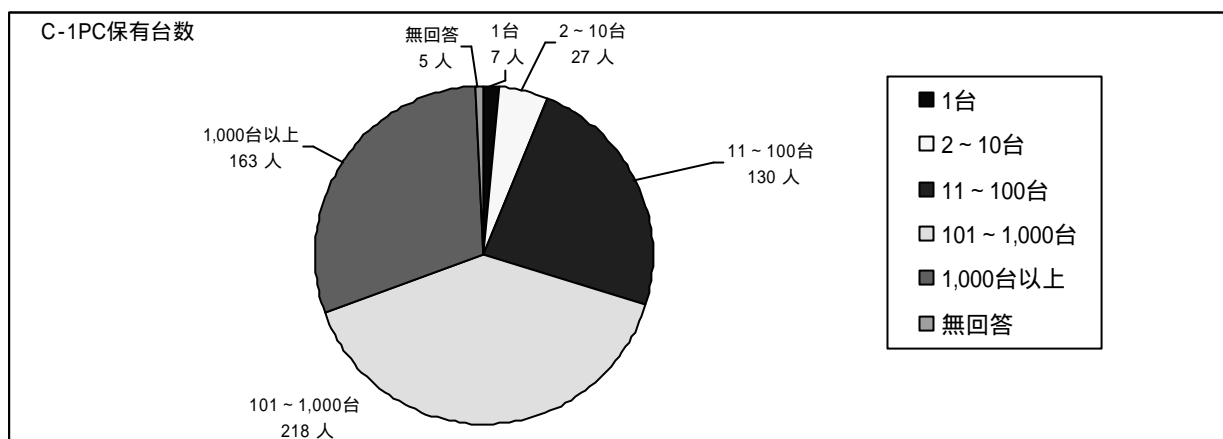


図4-9 C-1 保有コンピュータ台数分布

2.3.2. インターネットへの接続方法

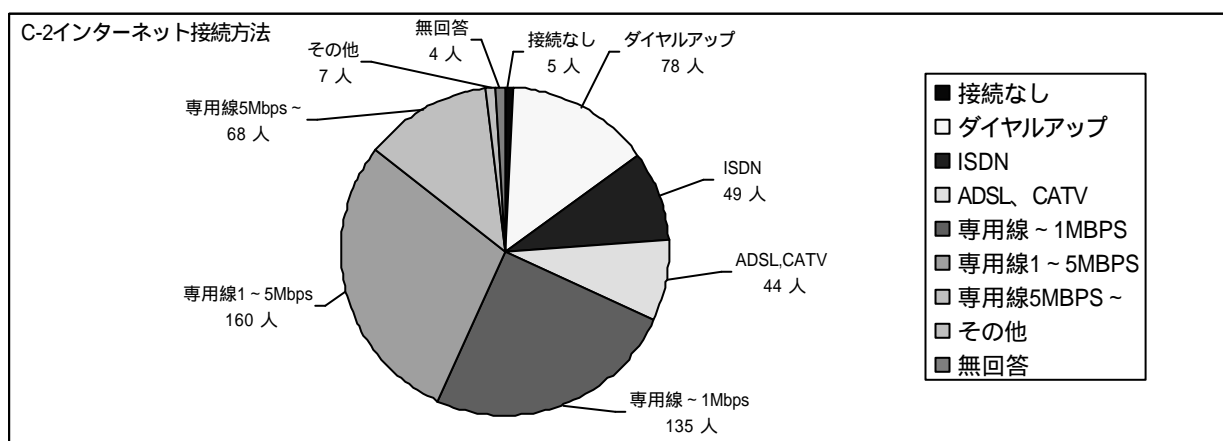


図4-10 C-2 インターネットへの接続方法分布

2.3.3. LANの有無

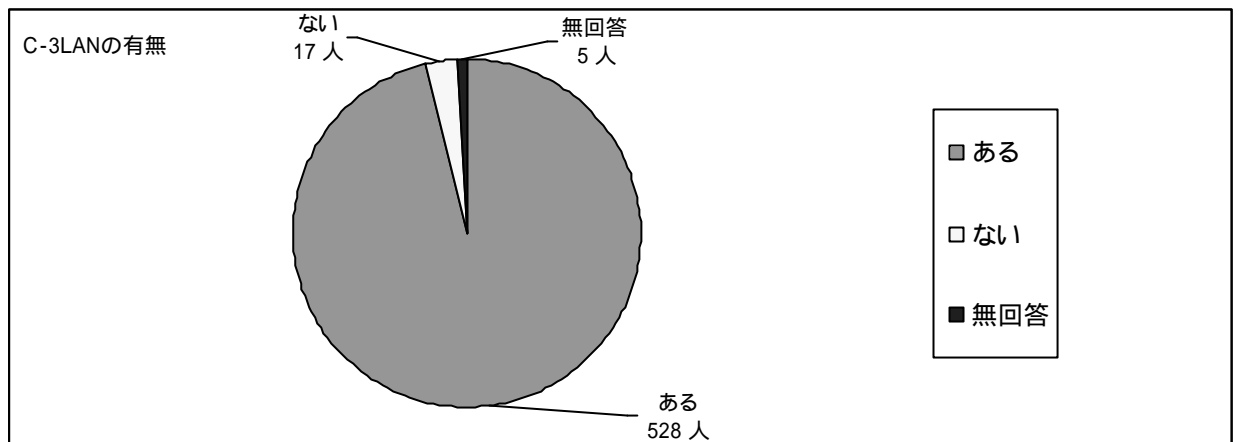


図 4-11 C-3 LAN 有無

第5章 分析結果

本章では、本調査の各調査目的から、調査目的を的確に表している設問を選択し、調査結果をグラフ化した。各グラフの数値の内訳等は、「第3篇 集計結果篇」の第1章に数値データを表として掲載した。

1. 全体傾向

企業規模別傾向

企業規模(売上、従業員数、拠点数、クライアントPC数)と情報セキュリティマネジメント(組織体制、技術導入)の相関関係の確認を目的とした。企業規模に関わらず、情報セキュリティ関連の技術導入は進みつつあるが、組織体制整備は企業規模が大きい場合のみ実施されているのではないかとの問題意識があったためである。

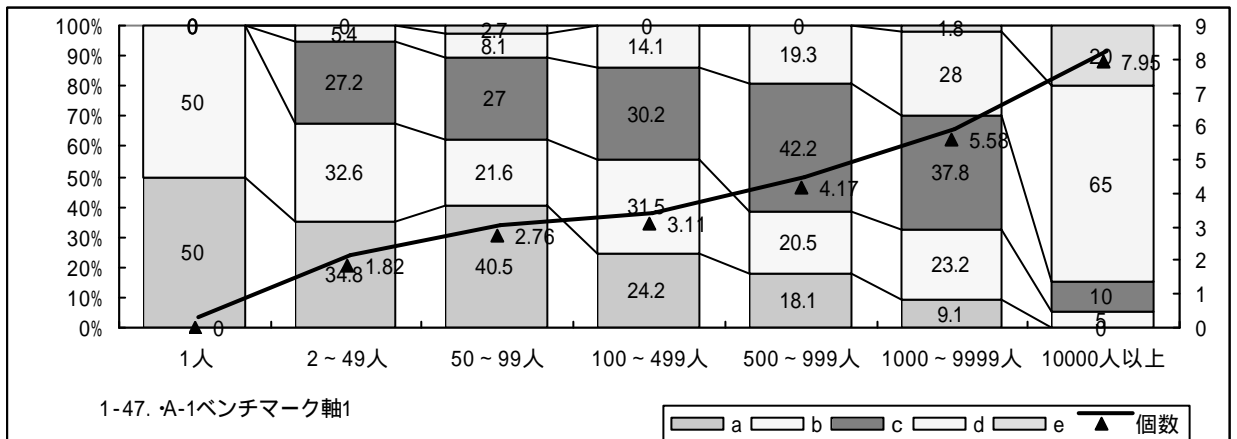


図 5-1 1-47 × A-1 体制整備状況と導入技術

図 5-1 の縦軸はベンチマーク軸 A (情報セキュリティ管理体制の整備状況) の点数を 5 段階に分けて表示している。この点数の内訳はベンチマーク点数の内訳として表 5-1 に掲載した。横軸は従業員数を表している。また折線グラフは問 1-47 (情報セキュリティへの体系的対策) における平均回答数を表している。縦軸の a~e は表 5-1 のとおりである。

表 5-1 ベンチマーク点数の内訳

	点数の幅
a	0 ~ 平均点/2 未満
b	平均点/2 以上 ~ 平均点未満
c	平均点以上 ~ 平均点 × 1.5 未満
d	平均点 × 1.5 以上 ~ 平均点 × 2
e	平均点 × 2 以上

図 5-1 のとおり、従業員数が多いほど、ベンチマークの点数が高かった。また、従業員数が多いほど情報セキュリティへの体系的対策も進んでいることが分かった。

業種別傾向

業種と情報セキュリティマネジメント(組織体制、技術導入)の相関関係の確認を目的とした。これは、情報システムサービスを提供している情報処理業種、テロの対象となるおそれのある重要インフラストラクチャー業種とその他の業種では、情報セキュリティマネジメントに差異があるのではないかという問題意識があったためである。

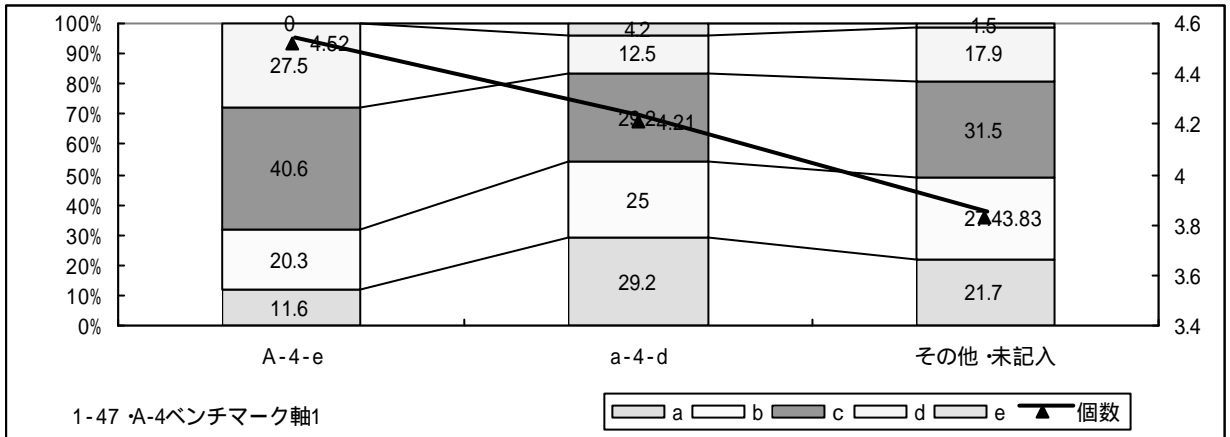


図 5-2 1-47×A-4 各業種別に見る体制整備状況と導入技術

本グラフの縦軸はベンチマーク軸 A (情報セキュリティ管理体制の整備状況)の点数を5段階に分けて表示している。横軸はA-4-eが情報・通信、a-4-dがエネルギー、その他・未記入を表している。また折線グラフは問1-47(情報セキュリティへのシステム的対策)における平均回答数を表している。縦軸のa~eは表5-1のとおりである。

情報・通信業界の特徴として、ベンチマークの点数の高さと情報セキュリティ関連技術の導入数の多さが挙げられる。エネルギー業界の特徴として、情報セキュリティ関連技術の導入数の多さが挙げられるが、ベンチマークの点数は平均程度であった。

2. 情報セキュリティマネジメントの実態把握

2.1. 情報セキュリティポリシーの整備状況

情報セキュリティポリシーの整備状況

近年、情報セキュリティポリシーの重要性についての認識は高まりつつある。そのため、企業規模や業種に関わらず全般的に情報セキュリティポリシーの整備が進みつつあるのではないかと考えた。

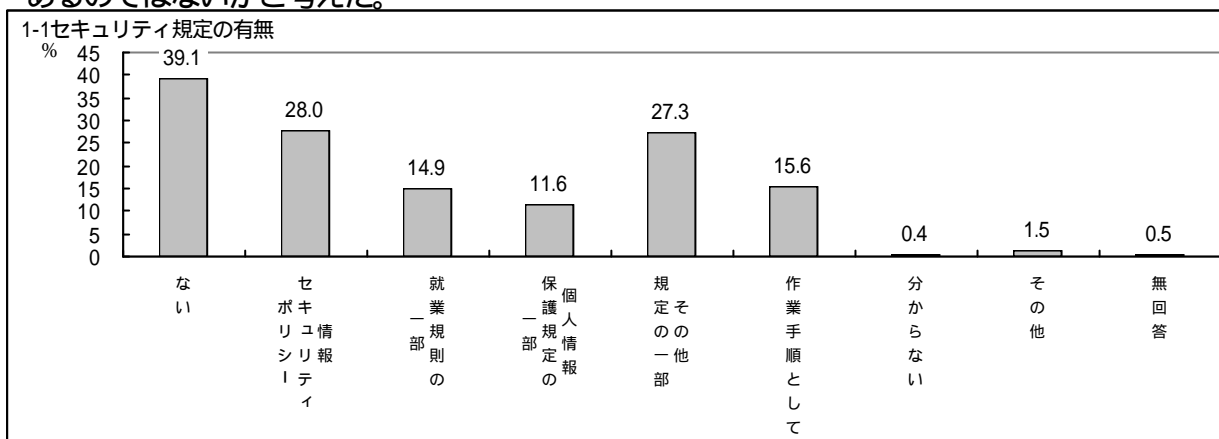


図 5-3 1-1 情報セキュリティポリシーの導入状況

情報セキュリティに関する規定を持たない企業が全体の39.1%だった。「情報セキュリティポリシー」を導入している企業は28%、作業手順を含めて情報セキュリティ関連の規定を定めている企業は15.6%であった。

情報セキュリティポリシーの整備は、特に重要インフラ業種や情報産業で進んでいるのではないかと問題意識から業種別の内訳を確認した。

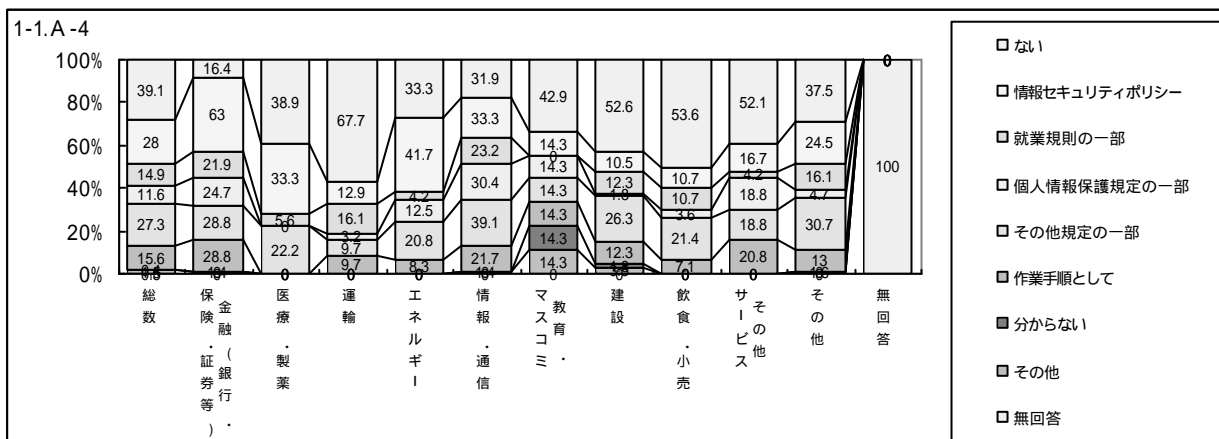


図 5-4 1-1×A-4 情報セキュリティポリシーの導入状況 (業種別内訳)

上記の予測どおり 他業種と比較して金融(63%)、医療・製薬(33.3%)、エネルギー(41.7%)、情報・通信業界(33.3%)の4業界で「情報セキュリティポリシー」を制定している企業の割合が高かった。

情報セキュリティポリシーの制定目的とその有用性

情報セキュリティポリシーを制定する企業は増えつつある。しかし、「責任体制の明確化」といったポリシーの本来の目的が失われているのではないかとの問題意識があった。

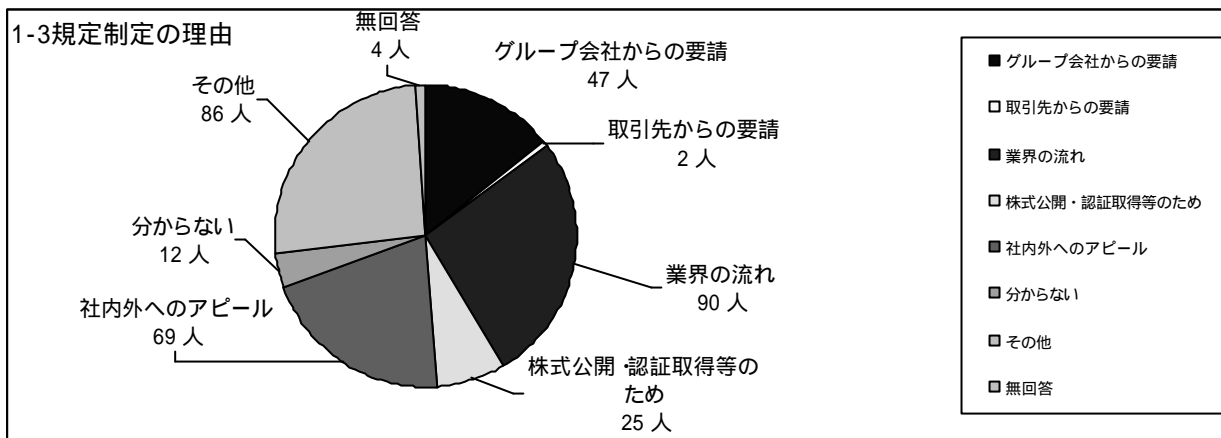


図 5-5 1-3 情報セキュリティポリシー制定目的

情報セキュリティポリシー制定の理由は、「グループ会社からの要請」、「取引先からの要請」、「業界の流れ」といった外的要因が41% (139人) だった。一方、「社内外へのアピール」、「株式公開・認証取得等のため」という内的要因は28% (94人) だった。

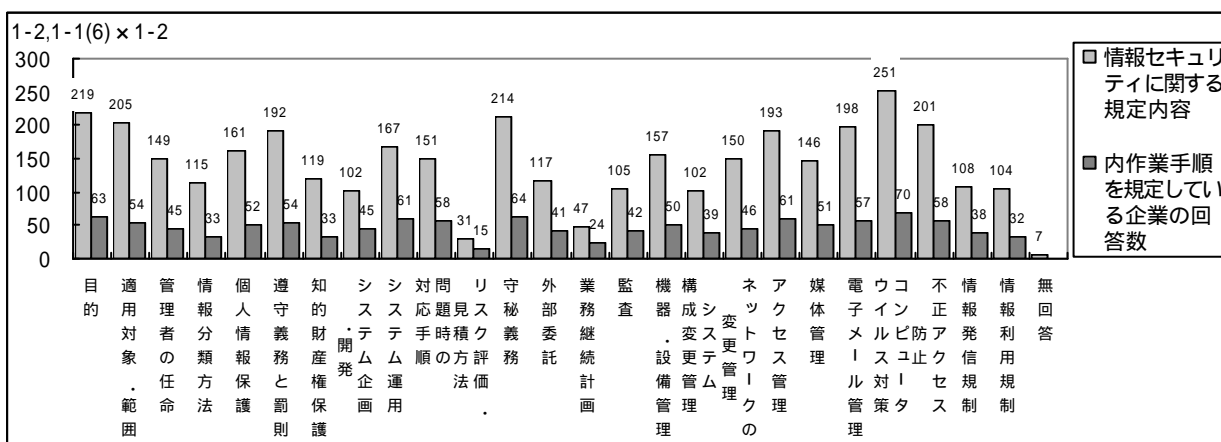


図 5-6 (1-2) 1-1(6) × 1-2 情報セキュリティプロシージャ(手順)制定状況

図 5-6 は、情報セキュリティに関する規定で定められている内容の全体回答と、情報セキュリティ関連の作業手順を有する企業の回答を掲載している。

情報システム機器管理やシステムの企画・運用等の情報システム関連のハード資産保護を主眼とした規定を持つ企業が多いことが分かった。ハード資産保護以外では、「ウイルス対策」を定める企業が多かった。しかし、予想に反して情報セキュリティ関連規定を有する企業の約 45% で「管理者の任命」を規定で定めていた。

また、「監査」「業務継続計画」「リスク評価・見積り方法」を規定として定めている企業は少ないものの、これらを定めている企業では作業手順まで含めて規定を定めている割合が高かった。

情報セキュリティポリシーの運用体制

調査開始前、情報セキュリティポリシーを制定する企業は増えつつあると考えていた。しかし、同時に情報セキュリティポリシーの導入後にポリシーのメンテナンスを行っている企業は少ないのではないかと考えた。情報セキュリティポリシーは制定後に適宜メンテナンスを行い、現状に即した規定としなければ形骸化してしまう

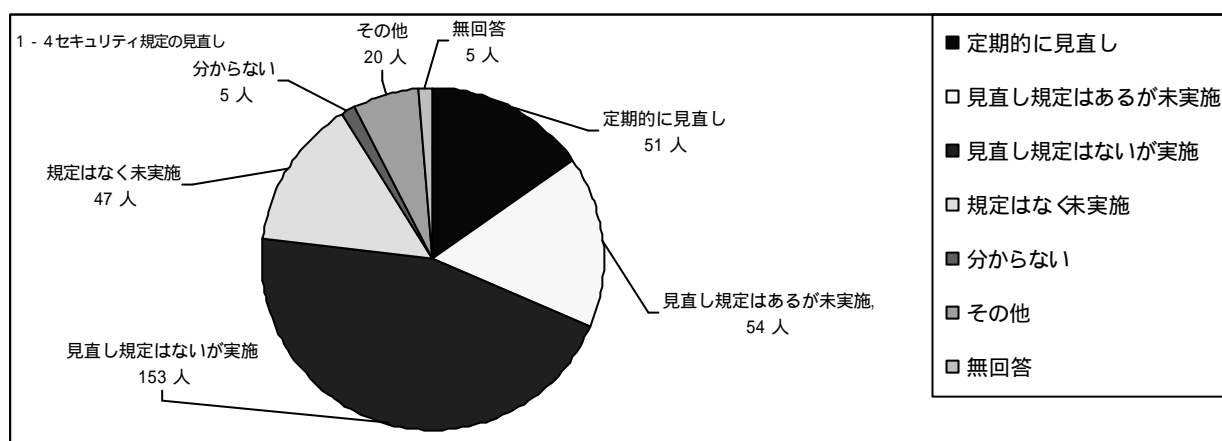


図 5-7 1-4 情報セキュリティポリシー運用状況

上記の予測に反して「定期的に見直し」をしている企業と「見直し規定はないが実施」という2つの回答を合計すると約61% (204人)の企業で定期的な改定を行っているということが分かった。

情報セキュリティポリシー未整備の理由

調査開始前、情報セキュリティポリシーの整備は進みつつあるものの、未整備の企業も多いと考えた。情報セキュリティポリシーは情報システムを利用してビジネスを行う場合の指針とも呼べるため、企業活動においてネットワークや情報システムの利用が進んでいる今日では、本来は業種・企業規模に関わらず全企業で必要である。情報セキュリティポリシーが未整備であるということは本来は経営者、業務担当者の理解不足が原因と思われる。しかし、回答では業界的・業種的に不必要だと認識している企業が多いのではないかと問題意識があった。

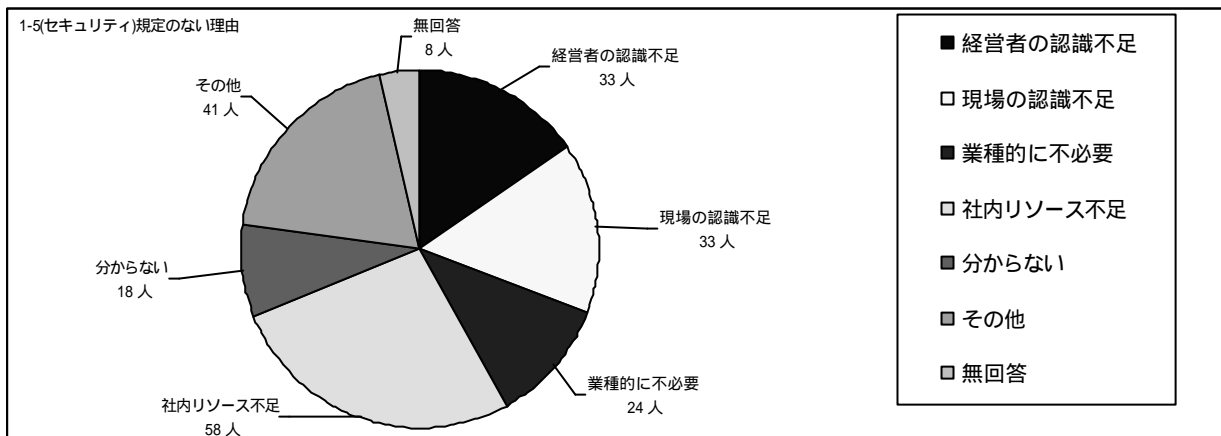


図 5-8 1-5 情報セキュリティポリシー未整備理由

「業種的に不必要」であるとの回答は約 11% (24 人)であった。組織体制として「社内のリソース不足」であるとの回答が約 27% (58 人)、「経営者や現場の認識が不足」しているとの回答が約 31% (66 人)であった。

特に必要性の認識が低い業界はどこかを確認するため業種別内訳を確認した。

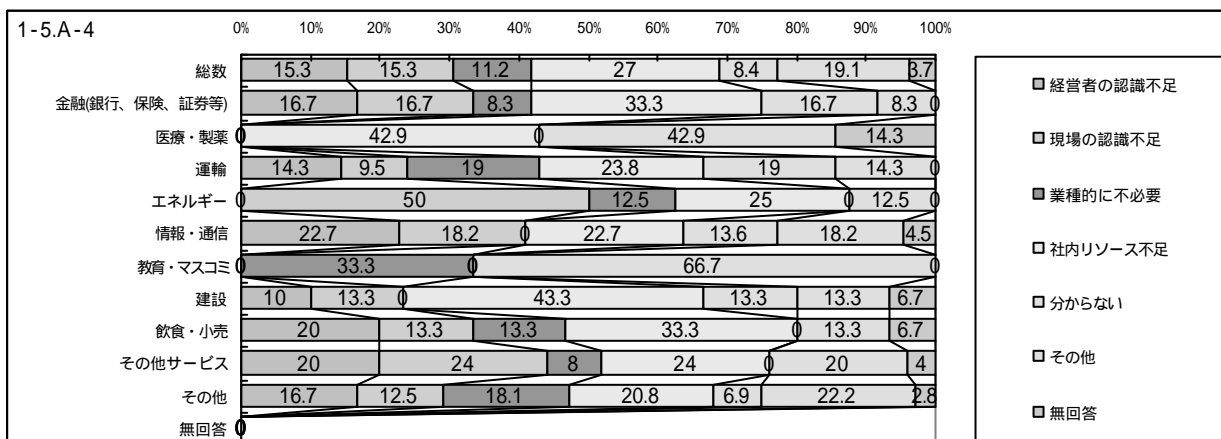


図 5-9 (1-5)(A-4) 情報セキュリティポリシー未整備理由 (業種別内訳)

「業種的に不必要」であるとの回答は、教育・マスコミと運輸業界で多かった。反対に、医療・製薬、エネルギー、情報・通信の3業界では「業種的に不必要」であるとの回答率が低かった。

2.2. 情報セキュリティ管理体制の整備状況

情報セキュリティ管理部門の設置状況

情報セキュリティへの認識が高い企業であっても、まだ日本では情報セキュリティの管理部門を専任で設置している企業は少ないのではないかと考えた。

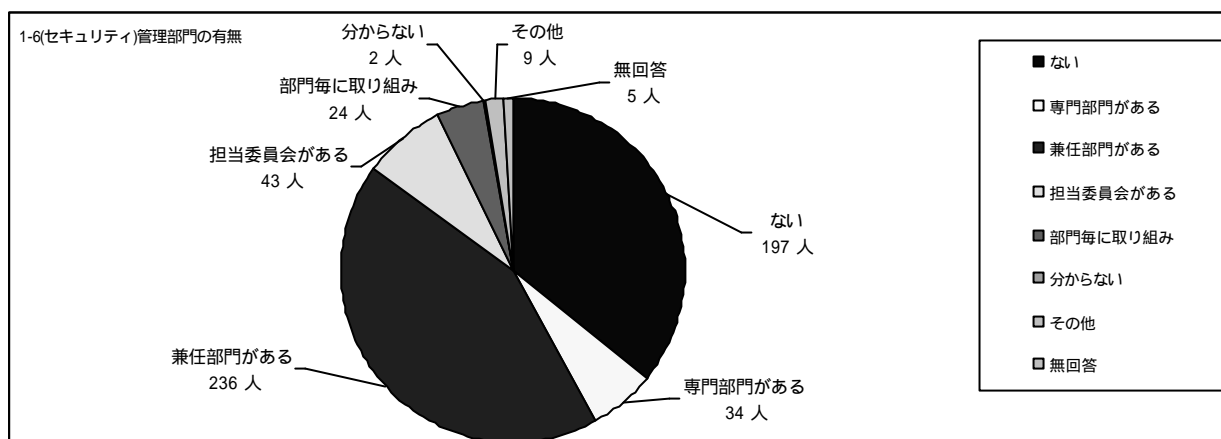


図 5-10 1-6 情報セキュリティ管理部門の設置状況

上記の予測どおり情報セキュリティに対応するための「専門部門がある」と回答した企業は約 6% (34 人)であった。「兼任部門がある」と回答した企業が最も多く約 43% (236 人)であった。また、情報セキュリティに対応するための部門が「ない」と回答した企業が約 36% (197 人)であった。

情報セキュリティ等リスクに対する規制や推奨のある業種等があるため、業種別に設置状況に差があるのではないかと考え業種別内訳を行った。

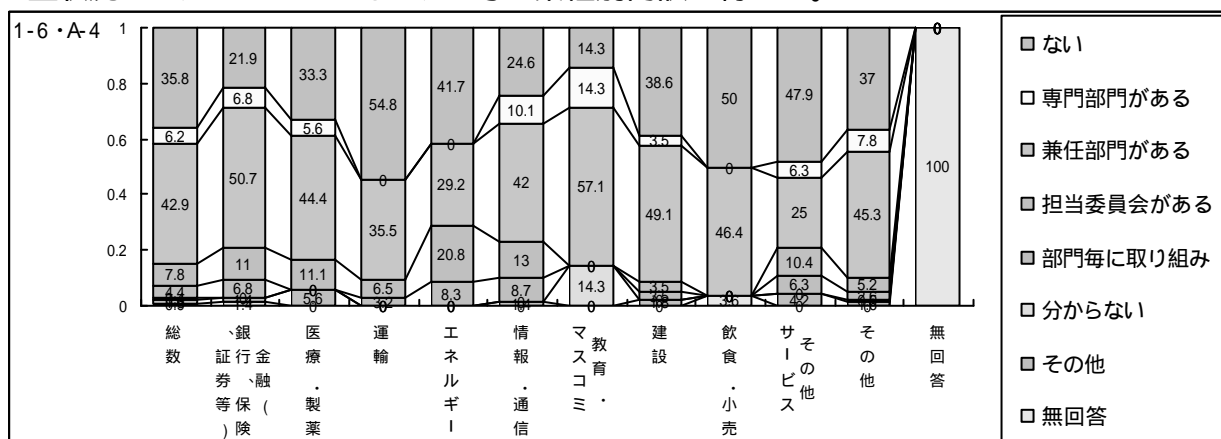


図 5-11 1-6×A-4 情報セキュリティ管理部門の設置状況 (業種別内訳)

情報セキュリティに対応するための「専門部門がある」と回答した企業は、教育・マス・コミ、情報通信、金融、医療・製薬の 4 業種で多かった。反対に、情報セキュリティに対応する部門が「ない」と回答した企業は、運輸、飲食・小売、その他サービス業界で多かった。

情報セキュリティ管理部門のリソース

調査前、情報セキュリティは、技術的な問題であると考える企業が多いと考えた。そのため、情報セキュリティを管理する部門では情報システムの技術者を中心とした人材配置を行っているのではないかと考えた。

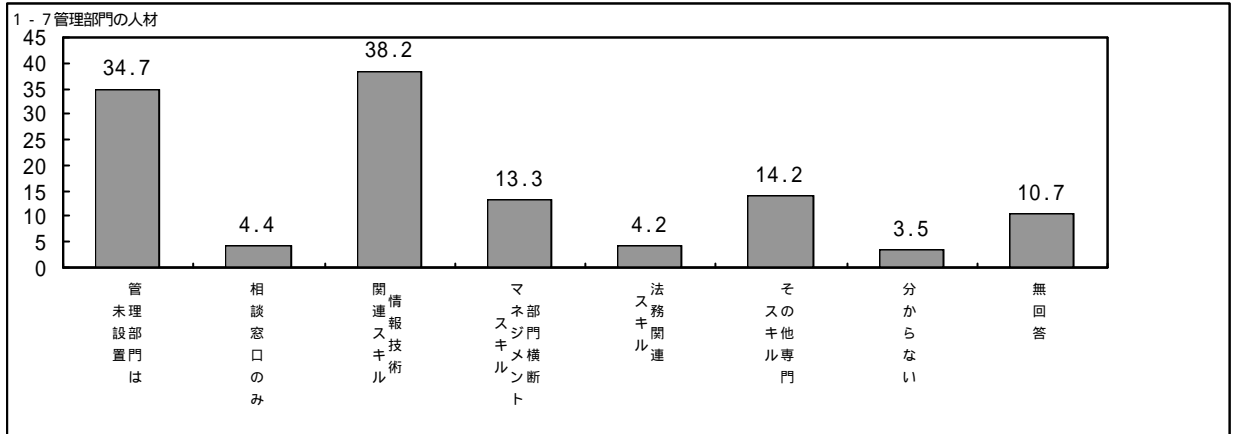


図 5-12 1-7 情報セキュリティ管理部門の人材

上記の予測どおり 情報セキュリティ対策を行う部門に配属されている人材が保有するスキルの割合の中では「情報技術関連スキル」が最も高かった。部門横断マネジメントスキルや「法務関連スキル」を有する割合は少なく、情報セキュリティが技術的な問題として受け止められている現状が理解できる。

情報セキュリティ管理を情報システム関連技術中心に考えるため、組織的なマネジメントがおろそかになっているのではないかと考えた。これが、現在組織的なマネジメントと情報システム技術両方を供えた人材が不在なために発生しているのか、そもそも情報セキュリティの担当部門にはマネジメントスキルを求めているのかを明らかにするため、現状ではなく本来情報セキュリティ対策部門の管理者にはどのような経験を求めるべきかについて確認をした。

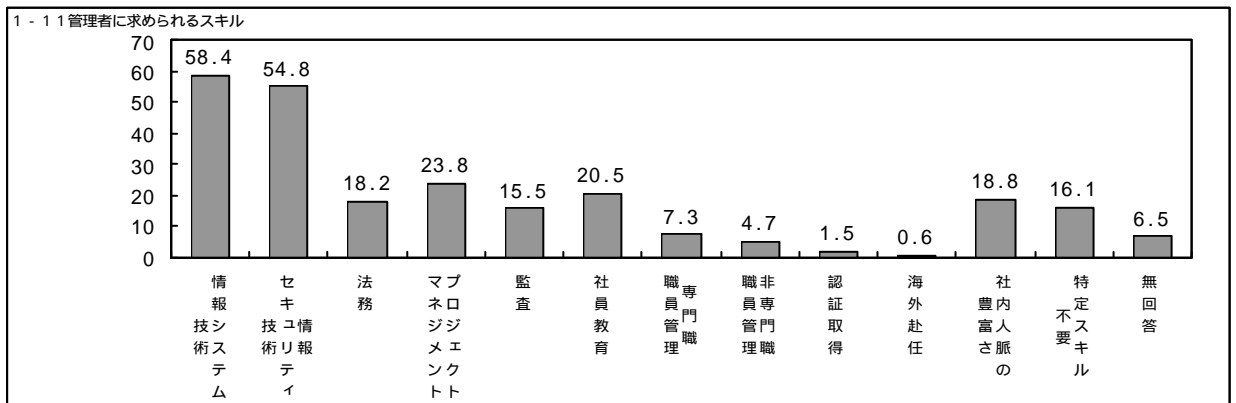


図 5-13 1-11 情報セキュリティ管理者の経験要件

上記の予測どおり情報セキュリティ管理者に求める経験は「情報システム技術」や「情報セキュリティ技術」が多く、情報セキュリティ管理者に「プロジェクトマネジメント」

や人材マネジメント経験を求める企業は少なかった。また「法務」「監査」といった対外的にも情報セキュリティが確保できているかどうかをモニタリングし説明責任を担うという役割を期待している企業が少ないことが理解できる。

本来、情報セキュリティを管理する部門は全社の情報資産を包括的に保護する部門であるため、部門横断的な権限が必要となる。しかし、現状では情報セキュリティは情報システム技術の一環と考えられており、情報システム部門の下に設定されているのではないかと考えた。

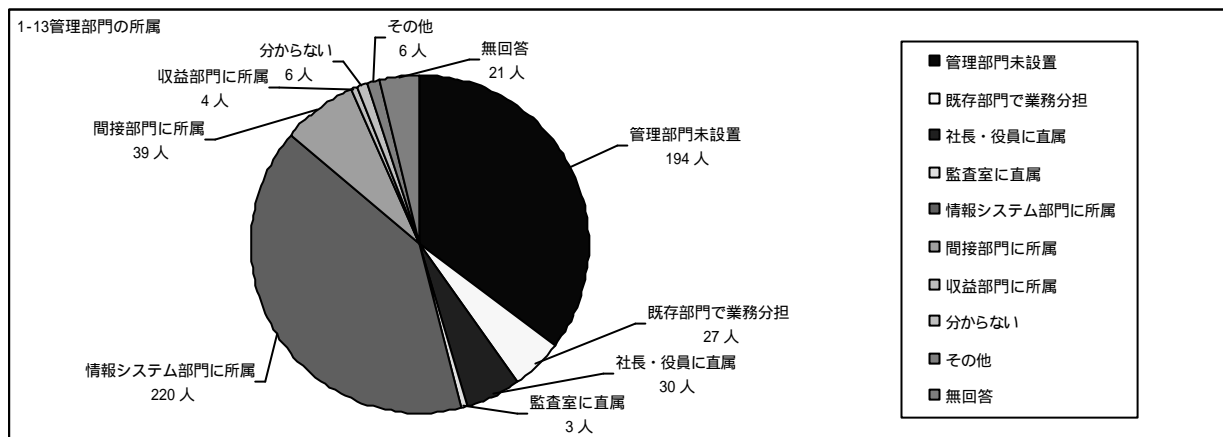


図 5-14 1-13 情報セキュリティ管理部門の所属

上記の予測どおり情報セキュリティ対策部門は「情報システム部門に所属」との回答が40%で最も多かった。部門横断的に業務を遂行可能な立場である「社長・役員に直属」している企業や「監査室に直属」している企業は少なかった。

情報セキュリティ管理者の有無

本来、情報セキュリティ管理者は全社の情報資産を脅威から保護するという役割のため部門横断的に権限を行使可能な役員クラスの任命が望ましい。しかし、現状としては情報セキュリティ管理者には情報セキュリティ技術を求め、部課長以下を任命している場合が多いのではないかと考えた。

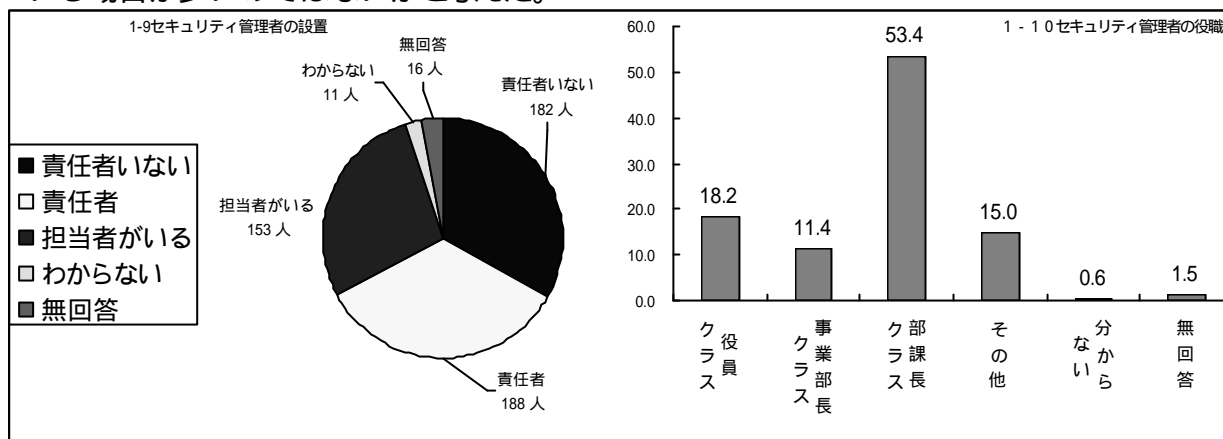


図 5-15 1-9×1-10 情報セキュリティ管理者の任命状況と役職

上記の予測どおり部課長クラスが 53.4%で最も多かった。

また、企業規模が大きいほど情報セキュリティ問題が発生した場合の責任の所在を明確にするため情報セキュリティ管理者が任命されているのではないかと考え企業規模別に任命状況を分析した。

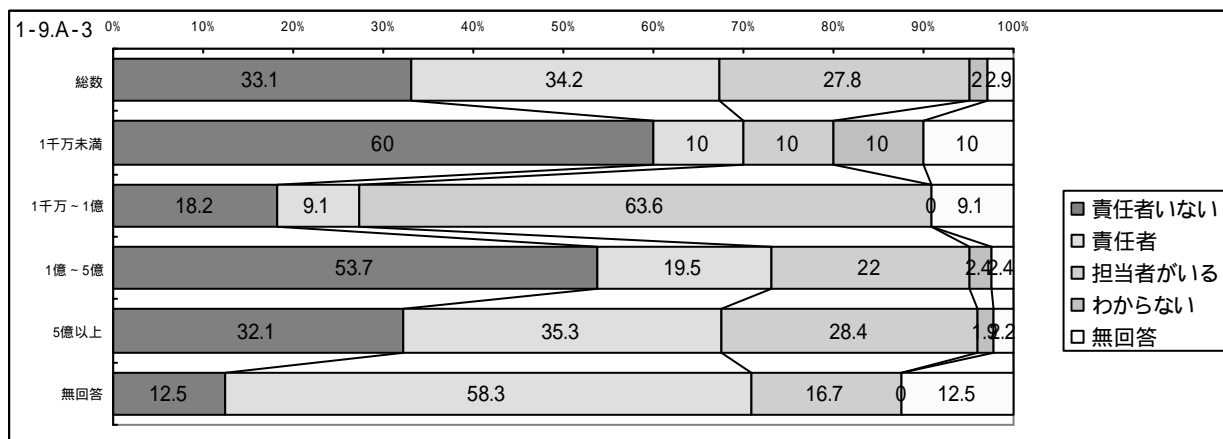


図 5-16 1-9×A-3 情報セキュリティ管理者の任命状況 (企業規模別内訳)

売上高 1 億円以上の企業では⁷⁸、企業規模 (売上高) が大きいほど情報セキュリティの「責任者がいない」との回答割合が減り「責任者がある」との回答割合が増加した。

⁷⁸ 売上高 1 億円未満の企業は母集団が少ないため比較対象外とした。

情報セキュリティ管理部門への連絡体制

情報セキュリティポリシー制定の目的の1つが、情報セキュリティ問題が発生した場合の連絡体制や対処方法の確立である。しかし、情報セキュリティポリシーを制定していながら、連絡体制は構築していない(または構築していても機能していない)企業が多いのではないかとの問題意識から連絡体制の有無を分析した。

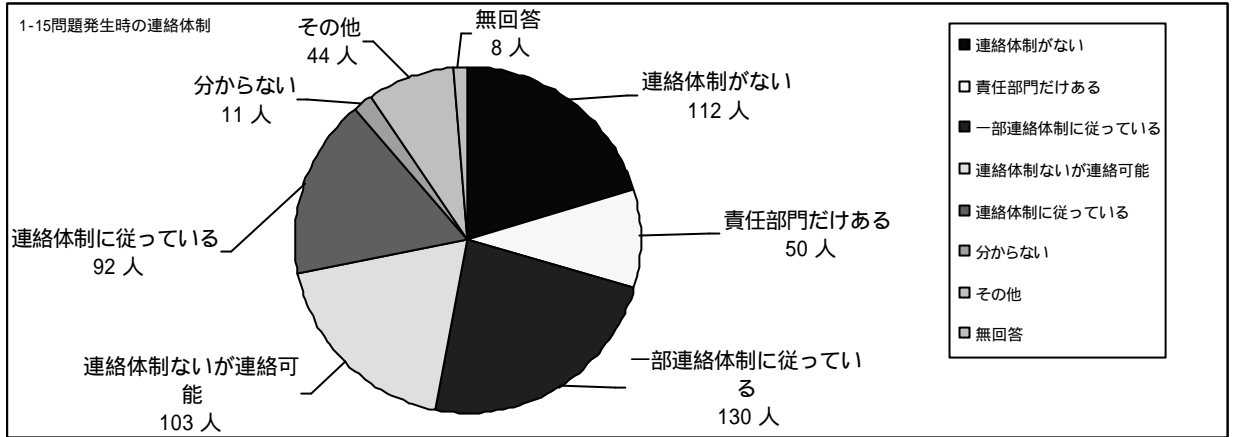


図 5-17 1-15 情報セキュリティ問題発生時の連絡体制

情報セキュリティ問題が発生した場合の「連絡体制がない」「責任部門だけあるが連絡体制は機能していない」との回答が約 29% (162 人) あった。しかし、何らかの方法で連絡が可能であると回答した企業が約 60% (325 人) であり、体制整備等は遅れているものの人的繋がりが等による草の根的な連絡体制が根付いている企業が多いと考えられる。人的流動が少ない場合、これらの人的ネットワークも有効だが今後の人材の流動化の動向を考慮すると「連絡体制はないが連絡は可能」と回答した企業でも組織的な体制整備を進めることが望ましいと考えられる。

また、連絡体制を構築している、と回答した企業であっても組織体制として構築・運用をしている企業は少ないのではないかと、明文化した連絡体制がないか、あったとしても連絡網のみという状況にはなっていないかとの問題意識から情報セキュリティポリシーでの規定状況と実際の行動をクロス集計し分析を行った。

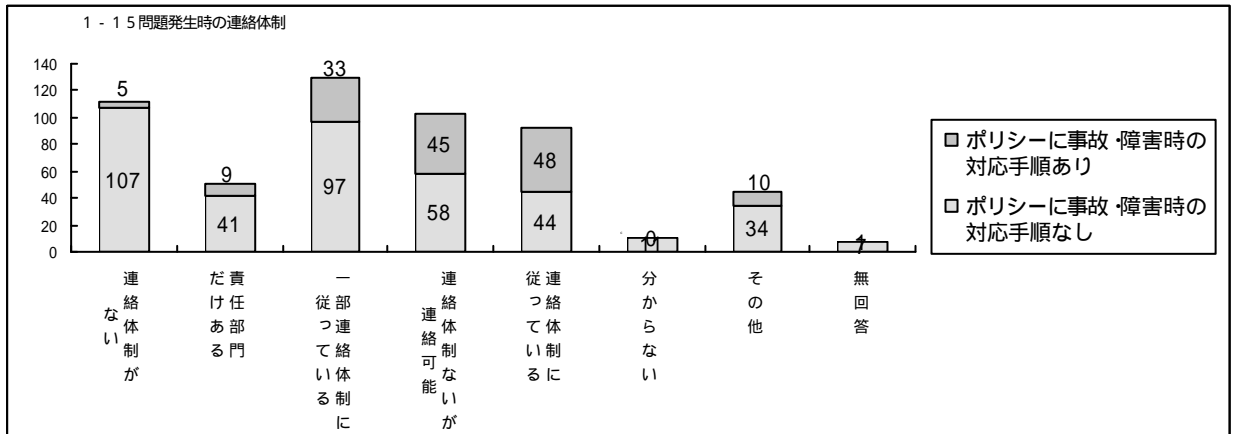


図 5-18 (1-2(10)X1-15) 情報セキュリティポリシーにおける情報セキュリティ問題発生時の連絡体制

図 5-18 のとおり、情報セキュリティポリシー上で情報セキュリティ問題が発生した場合の対応手順を定めている企業では、「連絡体制に従っている」との回答率が高かった。

業務継続計画

情報セキュリティ問題が発生した場合にどのように業務を継続するかという計画を予め決めておくことで、ビジネス及び関係者に与える影響を最小限に食い止めることが可能である。しかし、日本ではまだ業務継続計画を制定している企業は少数ではないか。また、例え定めていても連絡体制が中心で障害の切り分けや広報体制等は考慮していないのではないかとの問題意識から業務継続計画の有無を確認した。

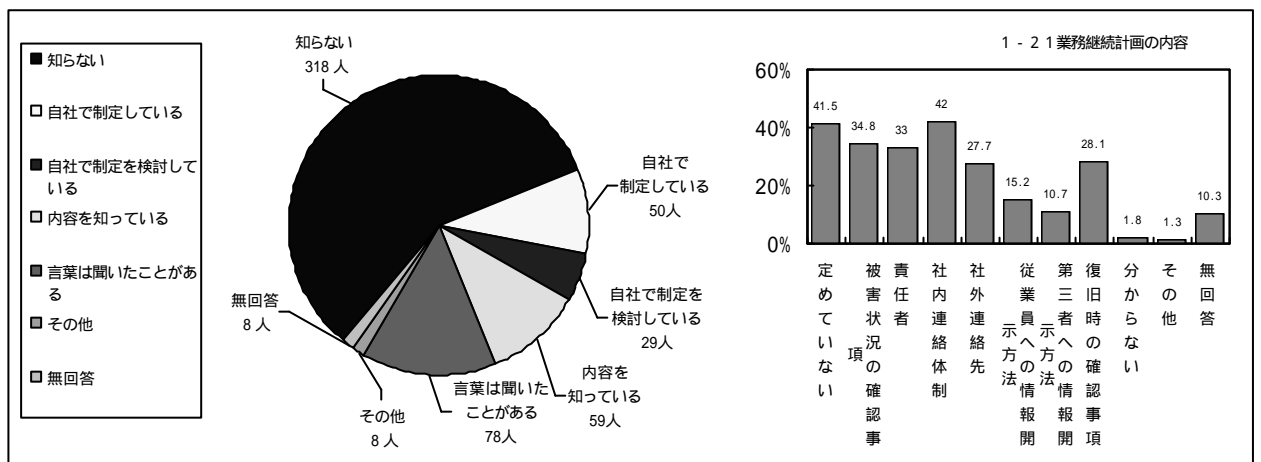


図 5-19 1-20 × 1-21 業務継続計画の対象

上記の予測どおり 業務継続計画という言葉自体を「知らない」と回答した企業が約 58% (318 人) と最も多かった。業務継続計画を「自社で制定している」と回答した企業は約 9% (50 人) であった。

業務継続計画で定めている内容を確認したところ、「社内連絡体制」(42%) や「被害状況の確認」(34.8%) といった連絡体制や被害状況の把握といった、問題をシステム的に回復するための対処方法が中心であることが分かった。一方、社内外に対する情報告知体制として「第三者への情報開示方法」や「従業員への情報開示方法」を定めている企業は少なかった。

2.3. 情報セキュリティ教育体制の整備状況

管理者教育

情報セキュリティ管理を円滑に行うためには、情報システム技術と組織横断的なマネジメント及びリスクに対する高い意識等広範囲に渡る能力が要求される。そのため欧米では、情報セキュリティ管理者が社外の専門機関が提供する講習を受講するといった方法で包括的な管理者教育を行っている。しかし、日本ではまだ情報セキュリティ管理者教育を計画的に実施している企業は少ないのではないかと、また、たとえ実施していたとしても、OJT が中心で包括的な情報セキュリティマネジメントを学ぶ機会は少ないのではないかとの問題意識から情報セキュリティ管理者教育の有無と内容についての分析を行った。

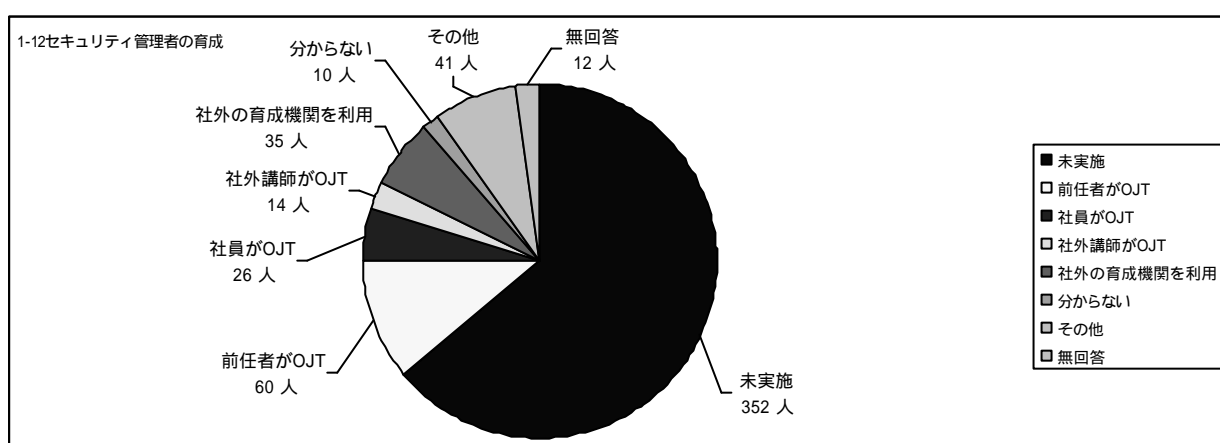


図 5-20 1-12 情報セキュリティ管理者教育

上記の予測どおり 情報セキュリティ管理者向け教育を「未実施」の企業が約 64% (352 人)であった。情報セキュリティ管理者教育を実施している場合は、OJT が中心であった。

全社員（情報システム利用者）教育

企業の情報資産を保護し有効に活用するためには、全社員が情報セキュリティやビジネスに関するリスク意識を向上させる必要がある。しかし、情報システム利用者全員を対象とした教育や啓発活動を実践している企業は少なく、技術職以外の一般社員が包括的な情報セキュリティを学ぶ機会が少ないのではないかとの問題意識から、全社員を対象とした情報セキュリティ教育の有無等についての分析を行った。

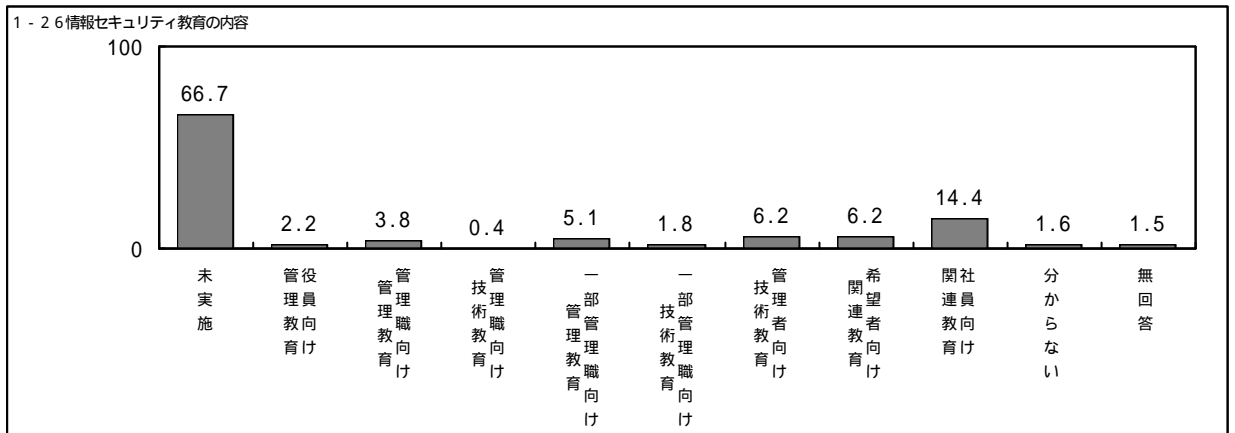


図 5-21 1-26 情報システム利用者教育

上記の予測どおり、情報システムの利用者を対象とした情報セキュリティ教育を「未実施」と回答した企業が66.7%であった。しかし「全社員向けの情報セキュリティ関連教育」を実施している企業も14.4%あった。

外部常駐社員、派遣社員教育

企業の情報資産を保護するためには、企業の正社員だけではなく情報資産にアクセスすることの可能な全員が情報セキュリティに対する意識を高めると同時に、問題を起こさないという明確な意思表示が必要である。そのため機密性の高い情報を扱う一部の企業では、外部から常駐社員を受け入れる際や派遣社員・アルバイトパート社員等を採用する場合には情報セキュリティの導入教育を実施した後で初めてネットワークにログイン可能なユーザ名とパスワードを発行するという手順を経ている。しかし、正社員を対象とした教育も怠りがちで、こうした外部社員等に対しては、機密保持契約の締結のみで、企業の実情に即した情報セキュリティ教育は実施していないのではないかとの問題意識があった。

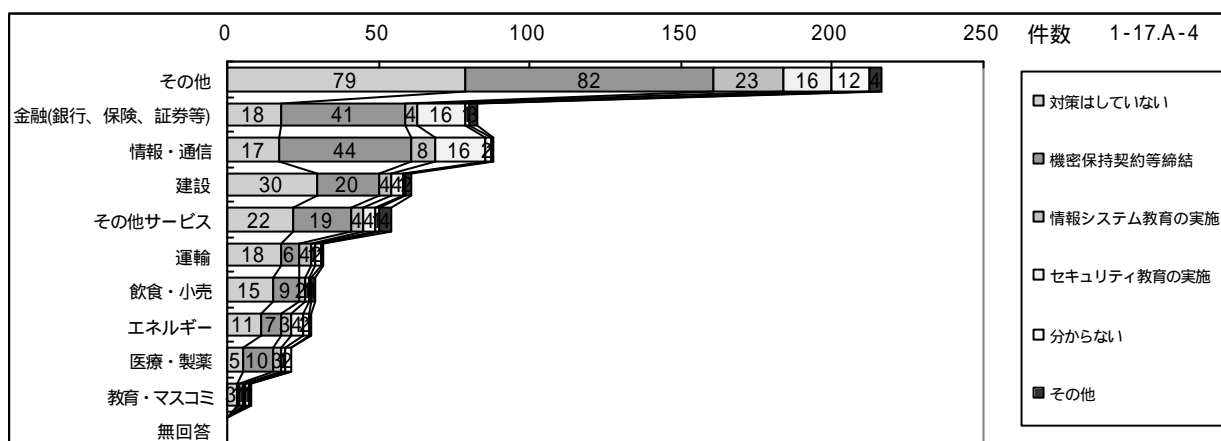


図 5-22 1-17×A-4 外部従業員受入時の対応 (業種別内訳)

上記の予測どおり 社外の人材に対して情報セキュリティに関する教育を実施している企業は少なかった。しかし、金融と情報・通信業界では情報セキュリティ教育を実施している企業の割合が他業種と比較して高かった。同様にこの 2 業種では「機密保持契約締結」を締結している割合も他業種と比較して高かった。

2.4. アクセス制御の実施状況

情報の重要度分類

情報セキュリティポリシー上で情報資産の重要度分類について明記しているかを確認した。また、実際にこの重要度分類のルールに則して情報資産を保管しているのかを確認した。

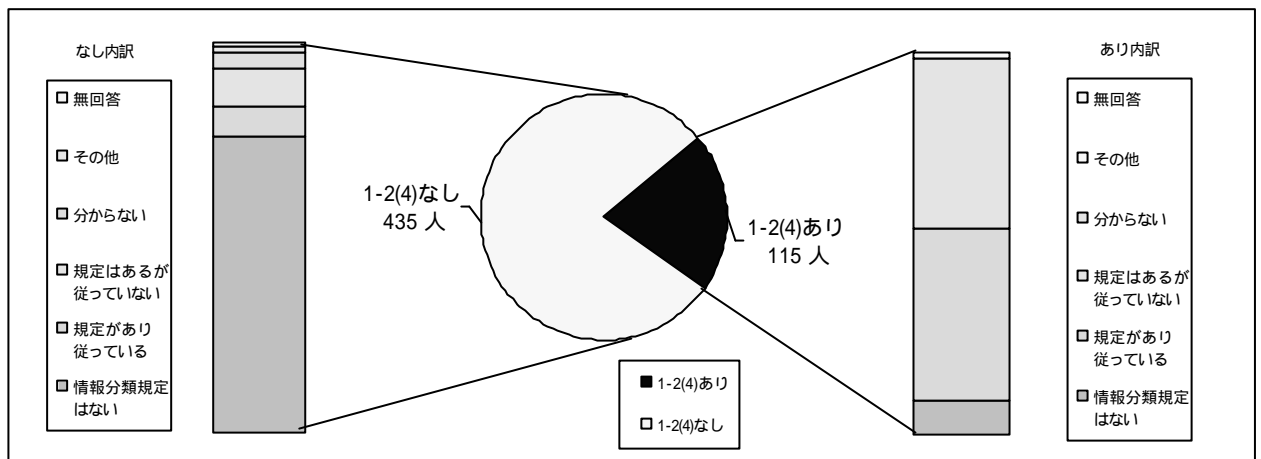


図 5-23 1-2(4) × 1-27 情報セキュリティポリシーにおける重要度分類有無と実情の比較

情報セキュリティの関連規定として「情報分類方法」を定めている企業は約 21% (115 人)である。該当企業の現状を確認したところ、「規定に従っている」との回答が約 52%と過半数であった。しかし、規定はあるものの従っていない企業が約 36%あった。

入退室管理

情報資産が設置されている場所に、入退室する人物名や目的、時間を管理することを入退室管理と呼ぶ。入退室管理は情報資産の保護に有効な手段である。しかし、企業の拠点数が少なく、全社員が既知の間柄の場合には、不審人物が企業内に無断で侵入した場合、発見が容易である。そのため、入退室管理が実施されることは少ないのではないかと、こうした意味からも、入退室管理は企業規模と関連があるのではないかと考えた。

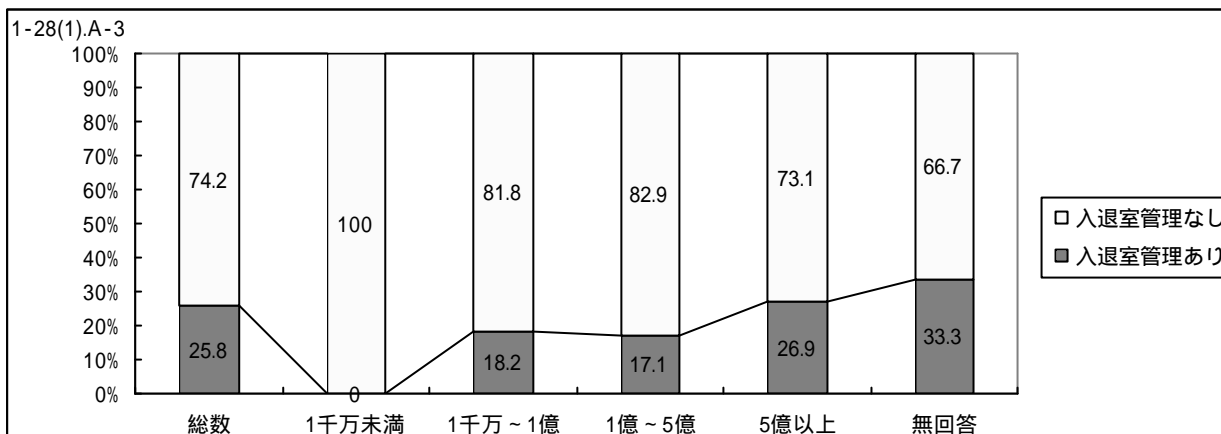


図 5-24 (1-28(1))A-3) 入退室管理企業 (企業規模別内訳)

上記の予測どおり、企業規模が大きくなるにつれて入退室管理を実施する企業の割合が増えていることがわかった。

また、入退室管理が監督官庁の検査項目となっている金融業等では入退室管理が進んでいるのではないかと考え、業種別の内訳を確認した。

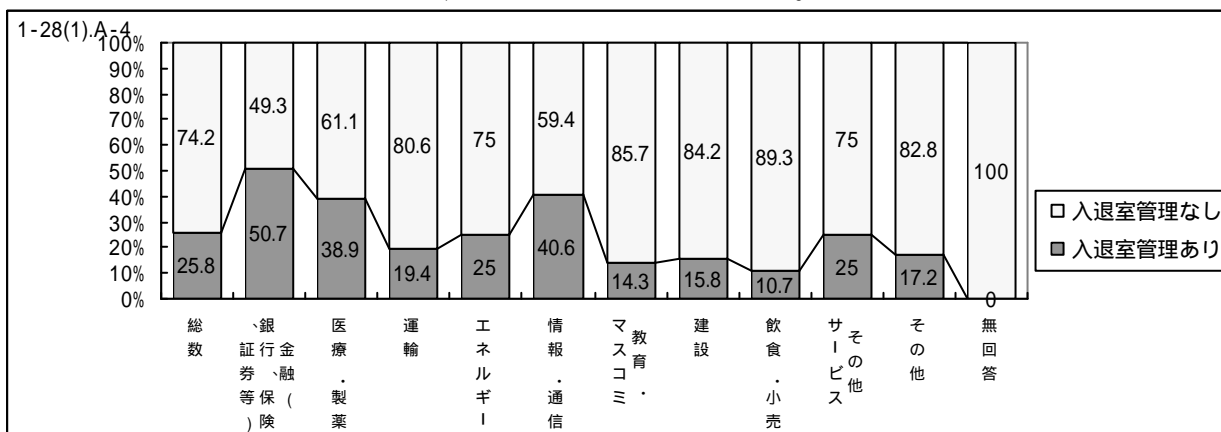


図 5-25 (1-28(1))A-4) 入退室管理企業業種別内訳

金融 (50.7%)、情報・通信(40.6%)、医療・製薬(38.9%)の3業種では「入退室管理あり」と回答した企業の割合が高かった。しかし、重要インフラ業種であるエネルギー業界では入退室管理を実施している企業の割合は全体の平均程度であった。

2.5. モニタリングの実施状況

サーバログの解析

重要な情報資産を保存しているサーバや社外と社内のネットワークの接続ポイントのアクセス状況を保存し、不審なアクセスについて解析することは情報セキュリティ問題の防止や発生後の対処として有効な手段である。情報セキュリティ管理部門の設置を行うことで、職務分掌が明確になり、サーバのアクセスログの解析のような定期的に継続して実施する必要のある業務を行うことができるようになるのではないかと考えた。そのため、定期的な解析を行うことで、情報セキュリティ問題を効率的かつ安全な段階で検知できているのではないかと考えられる。

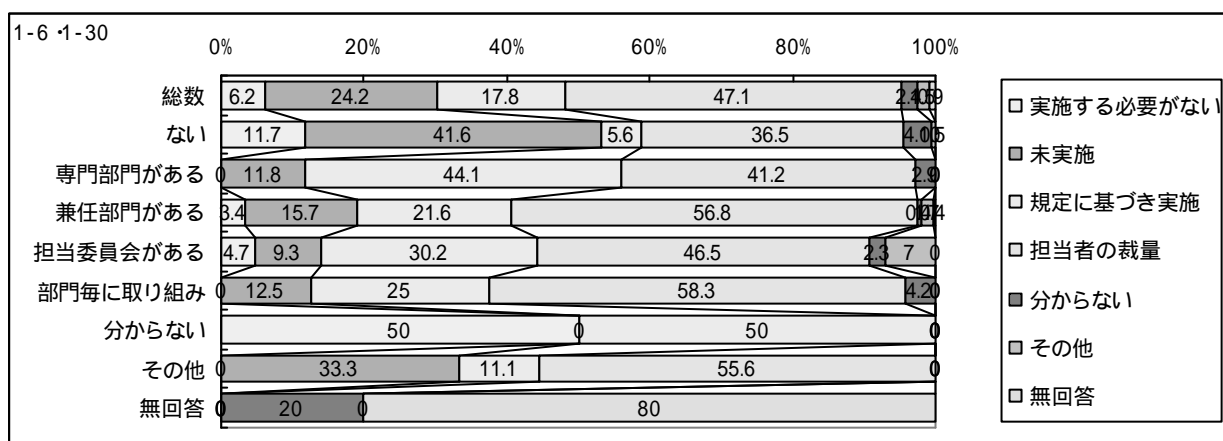


図 5-26 1-6×1-30 情報セキュリティ管理部門有無とアクセスログ解析の関係

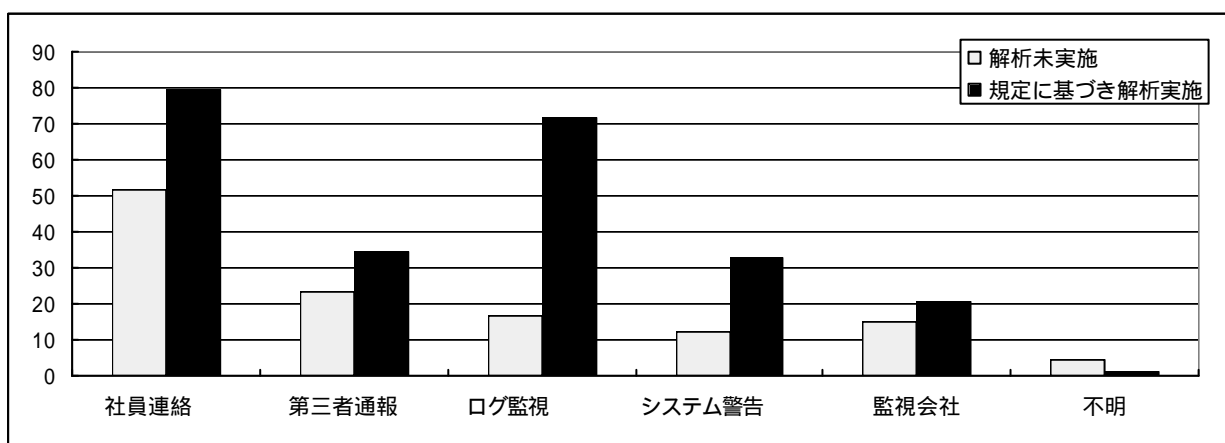


図 5-27 2-5×1-30 アクセスログ解析と情報セキュリティ問題認識方法

上記の予測どおり 図 5-26 では、情報セキュリティの専門部門がある「企業がアクセスログ解析を「規定に基づき実施」と回答した割合が 44.1% と最も高かった。また、図 5-27 のとおり、担当者の裁量ではなく規定に基づき定期的にアクセスログ解析を実施している企業は、アクセスログ解析を未実施の企業と比較して、情報セキュリティ問題の発見数が高かった。

サーバの最新状態の確保

情報セキュリティを確保するためには、情報システムの利用状況等のシステム的なモニタリング以外にも、定期的に確認すべき情報は多い。情報資産を保存するサーバのソフトウェアの最新状態を確保することは、既知のセキュリティホールを狙った攻撃からの保護という観点からも重要である。

そのため、情報のモニタリング状況の一例として、情報システム関連のパッチ等のリリース状況の情報収集を行い、適切に対処しているかについて質問した。

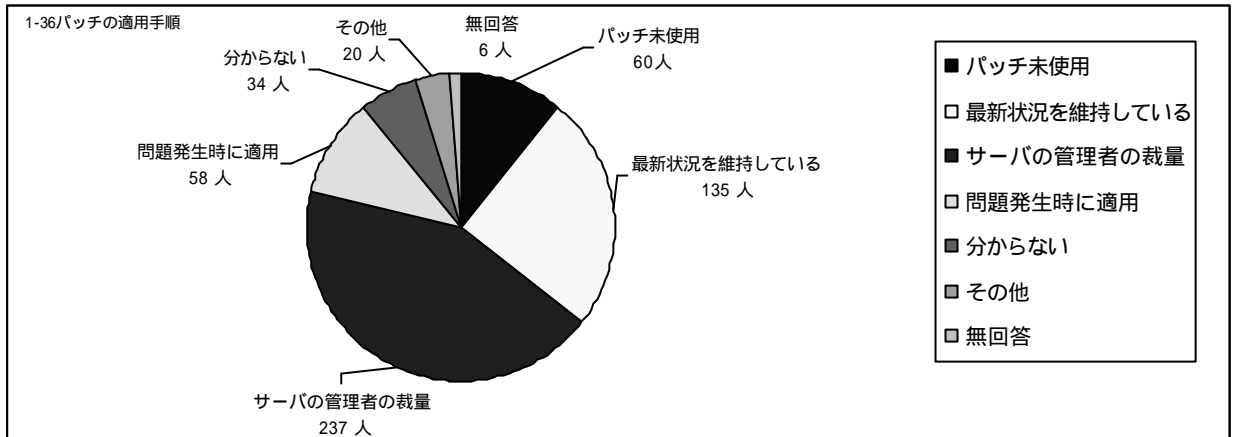


図 5-28 1-36 サーバへのパッチ適用タイミング

最新状況を維持しているとの回答は約 25% (135 人)であった。「サーバ管理者の裁量」で適用しているとの回答が約 43% (237 人)で最も多かった。

2.6. システム導入及び構成変更に関する安全性の確保状況

クライアントPCの構成変更

一般ユーザの技術が向上し、簡便な構成変更 (RAM メモリ増設、ハードディスク交換、アプリケーションソフトの追加削除等)を行うことのできるユーザが増えている。しかし、これらの行為は情報システム全体の効率を低下させる恐れや、アプリケーション等のライセンス違反を引き起こす恐れがある。情報システムの利用者が、こうしたリスクについての教育を受けていない場合にはポリシーや手順が策定されていても形骸化してしまう。そのため、クライアントPCの構成変更手順を確認した。

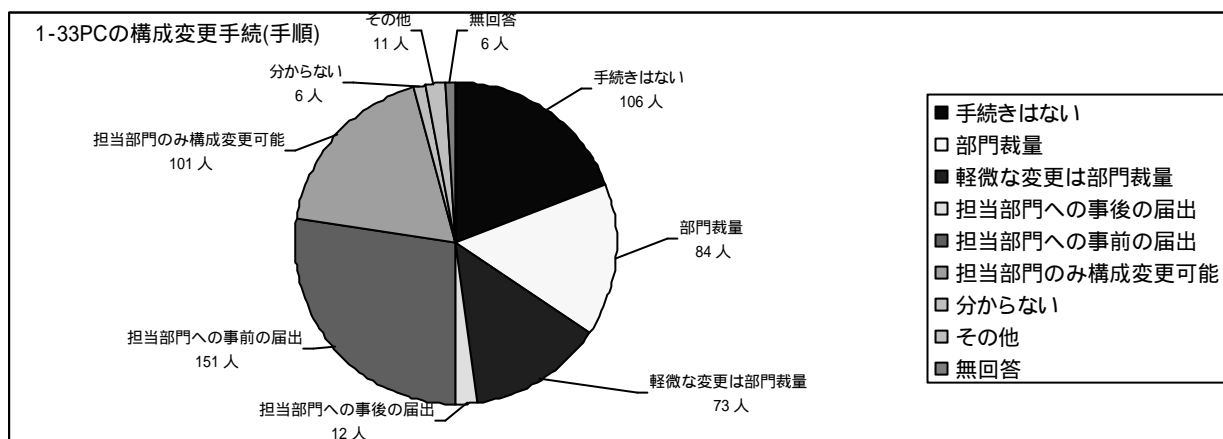


図 5-29 1-33 PCの構成変更手続

一般ユーザが利用しているPCの構成変更をするためには「担当部門への事前の届出」が必要。「担当部門のみ構成変更可能」との回答が約46% (251人)と約半数であった。しかし、一方で「手続きはない」と回答した企業が約20% (106人)であった。

また、情報セキュリティポリシーの制定、教育状況が情報システム利用者に与える影響を確認した。

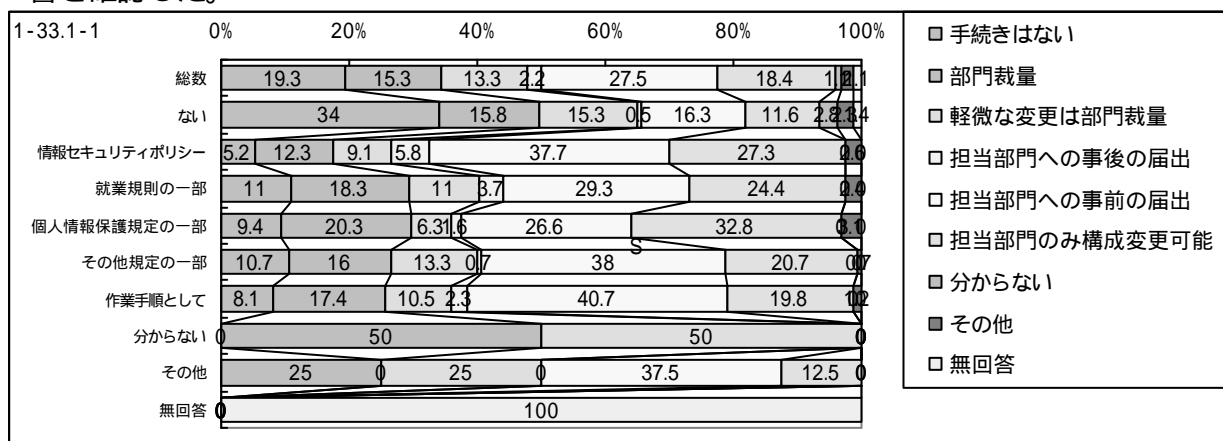


図 5-30 1-33×1-1 情報セキュリティポリシー形式別PCの構成変更手続

情報セキュリティポリシーを持つ企業では一般ユーザが利用しているPCの構成変更をするための「手続きはない」との回答が5.2%と他の企業と比較して低かった。また、

情報セキュリティ関連の作業手順を規定している企業は「担当部門への事前の届出」を必要とするとの回答が40.7%と、他企業と比較して高い割合であった。

ネットワークの構成変更

ネットワークの構成変更は、さまざまなシステム的な問題を引き起こす可能性がある。そのため、十分にテストを重ね、全社的な影響を考慮した上で実行する必要がある。

企業規模(拠点数)が大きくなるほど、別拠点で何らかの変更が加えられた場合に、連絡体制がない場合、問題が発生するまで変更の有無を検知することが難しくなる。そのため、企業規模(拠点数)が大きくなるほど体制整備が進められているのではないかと考えた。

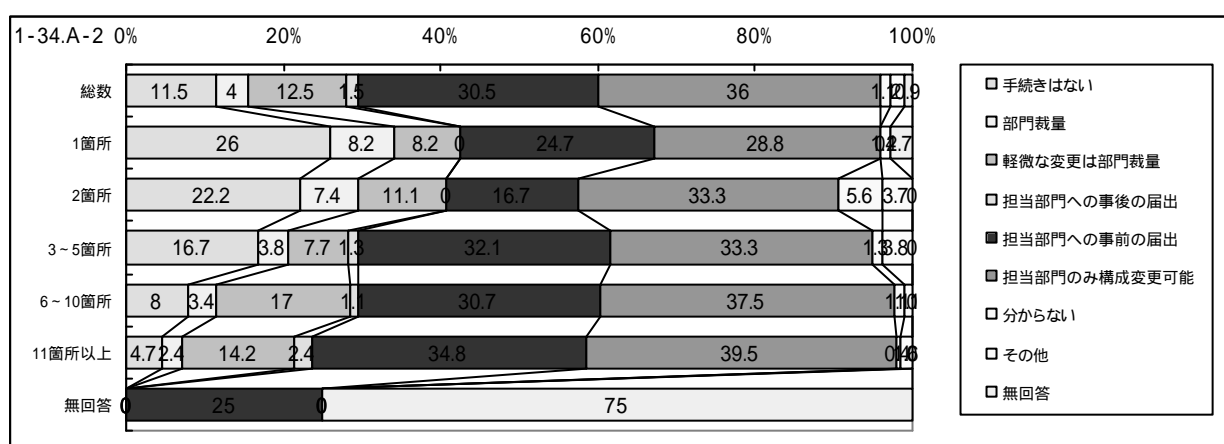


図 5-31 1-34 x A-2 ネットワークの構成変更手続(拠点数別内訳)

上記の予測どおり、ネットワーク構成の変更「手続がない」と回答した企業は、拠点数が増えるにつれて減少した。「担当部門への事前の届出」、「担当部門のみ構成変更可能」とも拠点数が増えるにつれて増加した。

サーバの構成変更

ネットワークの構成変更と同様にサーバの構成変更も、さまざまなシステム的な問題を引き起こす可能性がある。そのため、十分にテストを重ね、全社的な影響を考慮した上で実行する必要がある。

エンドユーザーコンピューティングが進むにつれて、ファイルサーバやプリンタサーバを各事業部で設置する企業が多い。しかし、こうした事業部等で設置されたサーバをダイヤルアップサーバとして設定し外部からのネットワークへの侵入を引き起こすことがある。そのため、サーバの構成変更に関する体制整備はエンドユーザーコンピューティングが進められ保有PCが多いほど進んでいるのではないかと考えた。

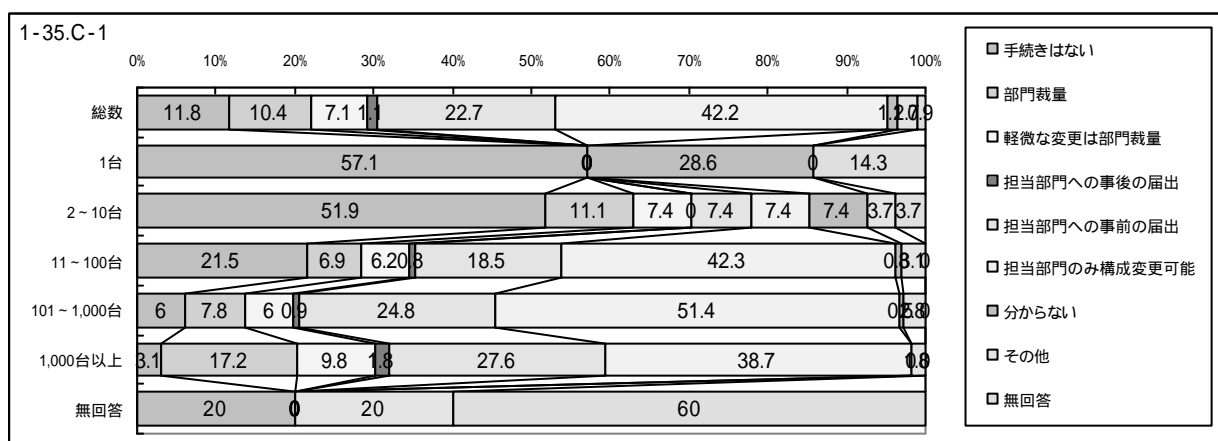


図 5-32 1-35×C-1 サーバの構成変更手続き (PC 台数別内訳)

上記の予測どおり 保有PC台数が増加するにつれてサーバの構成変更の「手続きがない」と回答した企業の割合が減少した。また、保有PC台数が増加するにつれてサーバの構成変更をするためには「担当部門への事前の届出」が必要であると回答した割合も増加した。

「担当部門のみ構成変更可能」であると回答した企業は101~1,000台までは保有PC台数が増加するにつれて増加したが、1,000台以上になると減少した。これは、ある一定規模以上の台数を超えると担当部門が直接変更を実施することが難しくなり届出制に留まるためではないかと推察できる。また、一定台数以上のPCを保有する企業では、PCを各事業部や各カンパニーの資産として計上し、管理も事業部内等で実施するケースが多いためではないかと推察できる。

情報システム関連の社内標準

情報システムの標準化を進めることで、システムの発生する問題の集約やリース・購入費用の効率化、情報システム利用者教育の効率化を進めることが可能になる。そこで、情報システム関連の社内標準に関する進捗度を確認した。

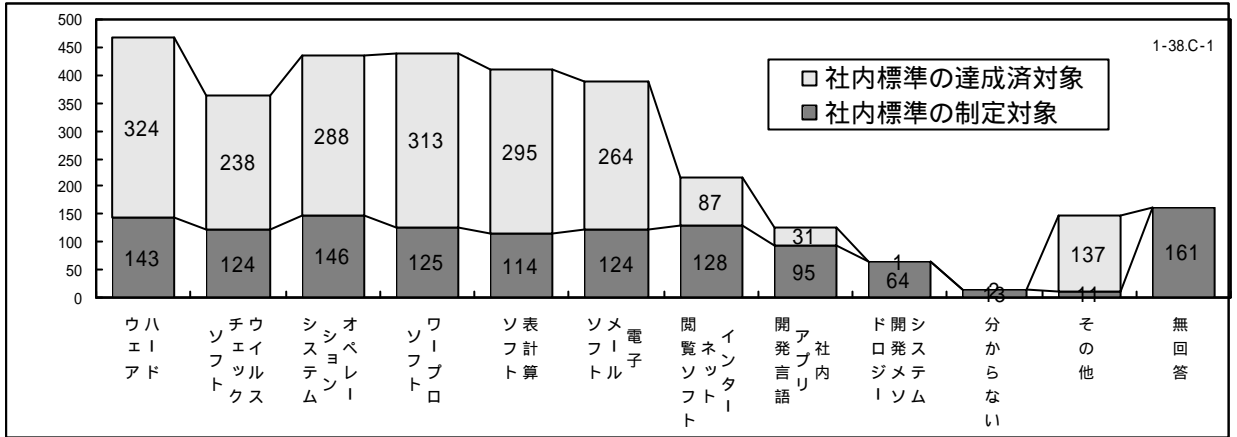


図 5-33 1-38 × C-1(c,d,e) 保有 PC11 台以上企業の標準化達成状況

図 5-33 は縦棒の高さが、対応するソフトやハードにおける社内標準の制定企業数を表す。縦棒の斜線部分が社内で 80%以上の標準化が実現している割合で、灰色部分が標準化が 80%未満である割合を表す。

社内標準を制定している対象としては「ハードウェア」「オペレーションシステム」「ワープロソフト」「表計算ソフト」「電子メールソフト」が多かった。標準化の実現割合が高い対象としては「ウイルスチェックソフト」「ワープロソフト」が挙げられる。社内データの交換(情報共有)の観点から、ワープロソフトの標準化を進めやすい一方、インターネットの閲覧ソフトや電子メールソフト等は異なるソフトを利用しているデータ交換自体は可能であるため進めにくいといえる。

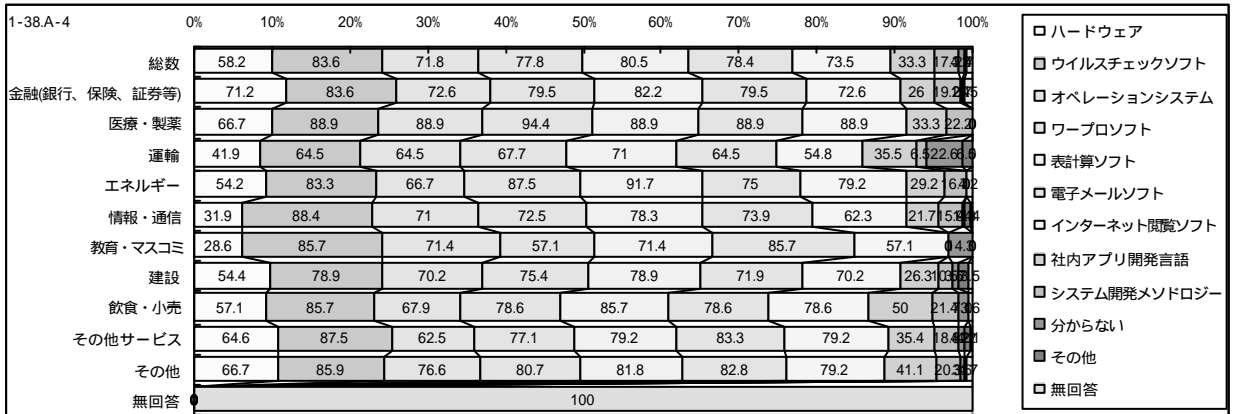


図 5-34 1-8 × A-4 標準化達成状況 (業種別内訳)

しかし、ビジネスアプリケーションの開発を行っている企業では、情報システムをクライアント環境に合わせる必要があり標準化を実施できないといった問題が考えられる。そのため、業種別の内訳を確認した。しかし、業種別内訳には差異は認められなかった。

2.7. アカウンタビリティの確保状況

システム監査、ペネトレーションテストの実施状況

第三者によるシステム監査や情報システムへの侵入テスト(ペネトレーションテスト：PT)を実施することで、情報資産に対する脅威と自社の対策レベルを客観的に把握することが可能になる。しかし、実際に実施している企業や実施結果の開示をしている企業は少ないのではないかと考えた。

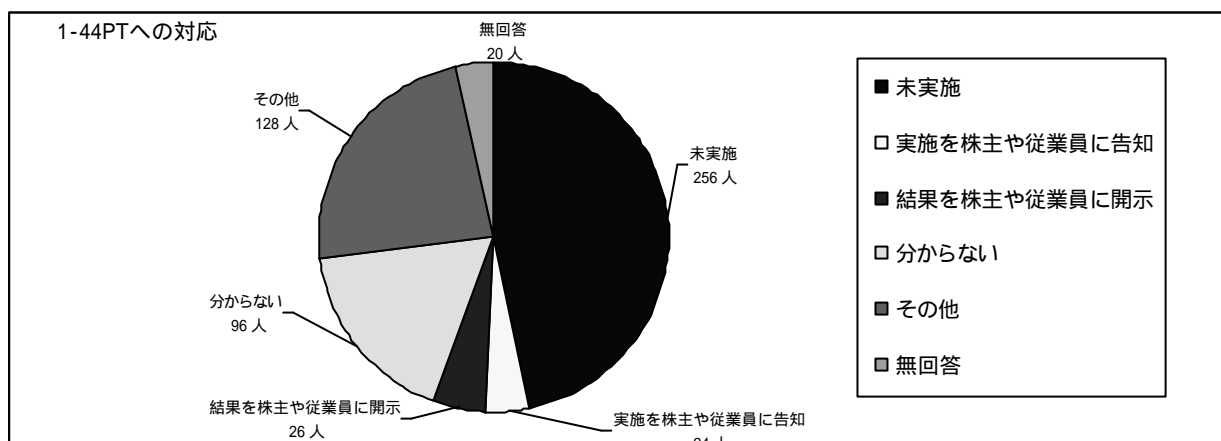


図 5-35 1-44 テスト結果への対応

上記の予測どおりシステム監査や侵入テストを「未実施」の企業が約 47% (256 人) と半数近くを占めた。一方、システム監査や侵入テストの「実施を株主や従業員に告知」したり「結果を株主や従業員に開示」する企業は約 9% (50 人) であった。

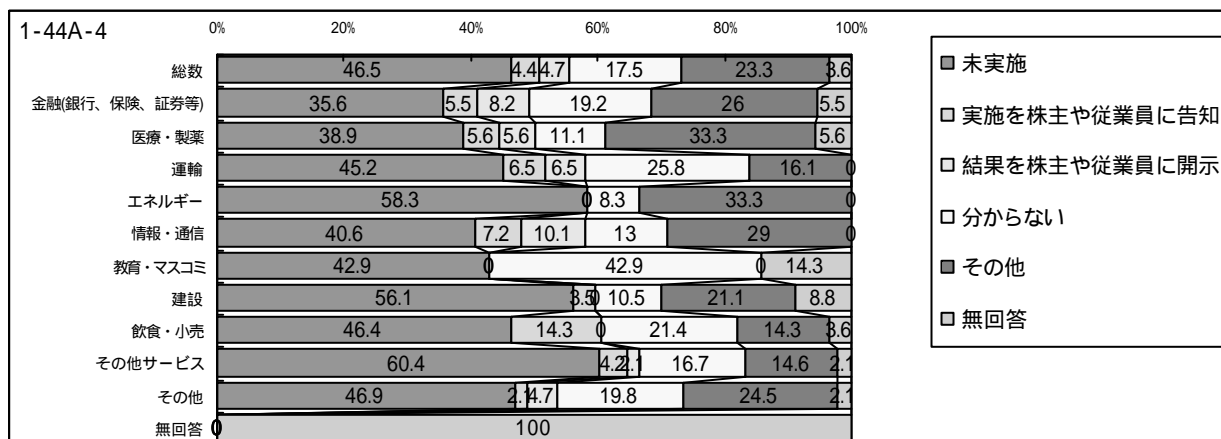


図 5-36 1-44 × A-4 テスト結果への対応 (業種別内訳)

金融機関では、金融庁により第三者によるシステム監査が推奨されている等、他業種と比較すると、こうしたテストに対する重要性に対する認識が高まりつつあると考えられる。また、医療 製薬業界も業界団体による情報交換フォーマットの取り決めを行う

等、情報セキュリティに対する意識が高いのではないかと考えられた。そのため、システム監査、ペネトレーションテストの実施は業界によって差異があるのではないかと考え業種別内訳を確認した。

上記の予測どおり金融(35.6%)、医療・製薬(38.9%)、情報・通信(40.6%)の3業種でシステム監査や侵入テストを「未実施」の企業の割合が低く、意識の高さが表れた。

業界動向、規制動向の把握

近年、情報セキュリティや個人情報保護に対する制度が整備されつつある。そのため、各企業は個人情報の保護や迷惑メールの配信規制等、情報セキュリティに関連する法令や指針に関する情報を収集し、自社に関連する場合にはこれらの指針等に準拠する必要がある。そのため、情報セキュリティ確保のための法令制定の動きや、業界における統一基準・標準制定の動きを把握しているかについて確認した。

また、情報セキュリティの確保が監督官庁の検査項目となっている金融業界や重要インフラ施設では、情報セキュリティの確保に特に注力しているのではないかと考えられたため業種別内訳を確認した。

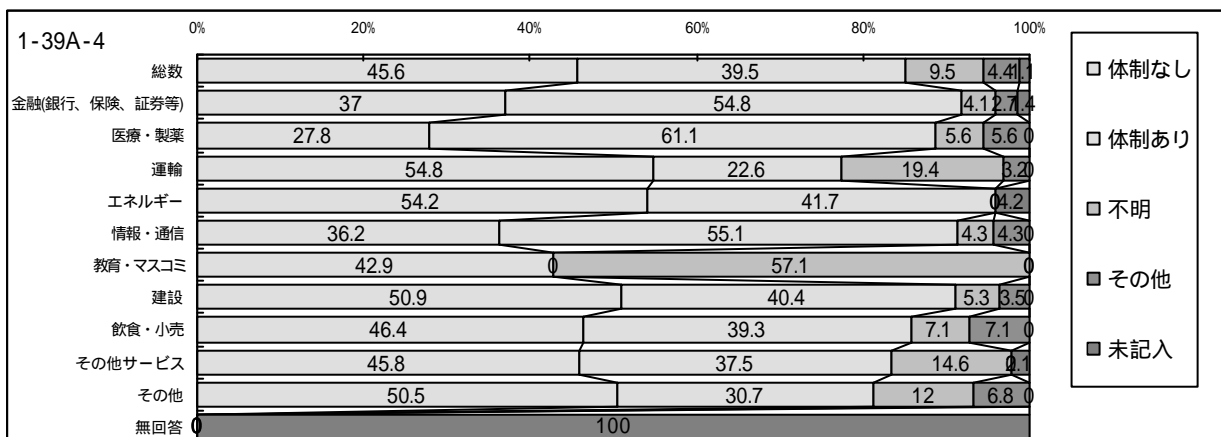


図 5-37 1-39×A-4 法令 業界動向の把握 (業種別内訳)

医療・製薬、情報・通信、金融の3業種で業界動向や規制動向の情報収集を行う体制を持つ企業の割合が高かった。

2.8. 情報セキュリティ管理のためのリソースの確保状況

情報セキュリティ対策のリソース有無

情報セキュリティを確保することで、企業の情報資産を保護し活用することが可能になる。情報資産は企業活動を行う上での知的資産であり、保護は必須である。しかし、日本では一般的に情報セキュリティの確保は情報システム技術の導入であり、情報システム部門の費用の一部で賄えば良いと考える経営者が少なくない。そのため、情報セキュリティを確保することを目的とした予算や人材を計上、確保している企業は少ないのではないかと考えた。情報セキュリティの確保にはコストが必要である。そのため各企業が、自社に見合った予算や人材確保を行っているかを確認した。

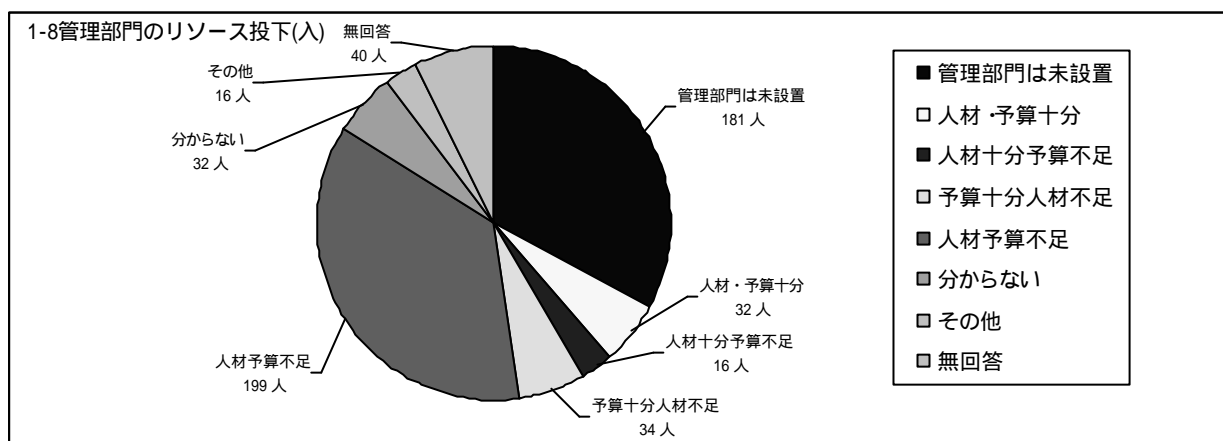


図 5-38 1-8 情報セキュリティ管理へのリソース配分

情報セキュリティを担当する部門を設置している企業では、「人材予算ともに不足」していると回答した企業が最も多かった。担当部門を未設置の企業もあるが、たとえ設置していても十分なリソースが確保できずにいる現状が理解できる。

情報セキュリティ予算の確保

第5章 2.8. で述べたとおり、情報セキュリティの確保は情報システム部門の業務の一部であると考えられる企業が多いため、情報セキュリティ対策のリソースは、情報システム部門のリソースを利用している企業が多いのではないかと考えた。

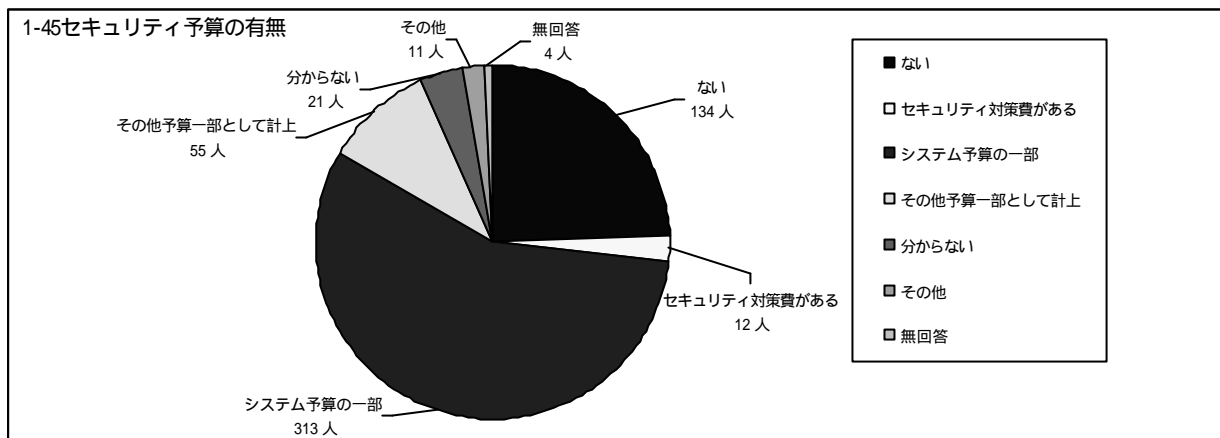


図 5-39 1-45 情報セキュリティ関連予算有無

上記の予測どおり、情報セキュリティ対策予算は「システム予算の一部」との回答が約57% (313人)であった。情報セキュリティの対策予算は「ない」と回答した企業が約24% (134人)、情報セキュリティ対策費として予算を計上している企業は約2% (12人)であった。

自社の情報資産に適した情報セキュリティポリシーの整備を行うことで、情報セキュリティとは技術だけではなく企業全体で取り組むべき問題であるとの認識が向上する。そのため、情報セキュリティポリシーを制定している企業の方が、情報セキュリティ予算の確保等のリソース確保が進んでいるのではないかと考えた。

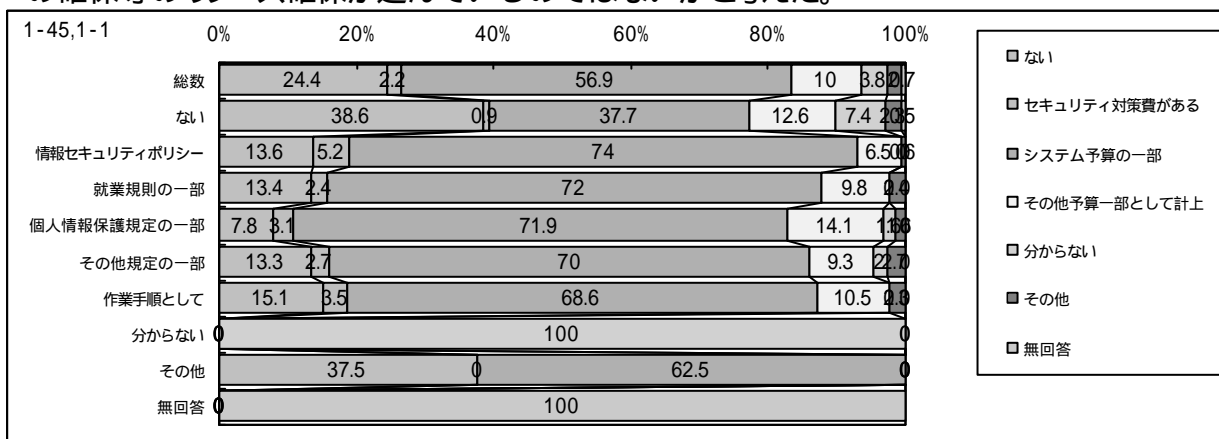


図 5-40 1-45×1-1 情報セキュリティ関連予算有無 (情報セキュリティポリシーによる予算有無別)

上記の予測どおり、情報セキュリティに関して何らかの規定を持つ企業は、規定を持たない企業と比較すると情報セキュリティ対策予算を計上している割合が多かった。情報セキュリティ関連規定の整備がリソースの確保の上でも重要であることが理解できる。

情報セキュリティ予算の対象範囲

アプリケーションソフトのバージョンアップ費用やウイルス定義ソフトのライセンス代等は、個別に見ると小額である。また、情報セキュリティに関する教育を行う場合も内部研修やセキュリティ対策ソフトや関連サービス会社が提供する無料研修が中心である。そのため、実際には人日コストは発生しているが支払い行為が発生せず、コストが見えにくいと言える。

しかし、企業規模(クライアントPC台数)が大きくなると、こうした目に見えない情報セキュリティ対策コストが膨大になる。また、事前に情報セキュリティ教育やバージョンアップを計画し重要性を告知していない場合、一般の情報システムユーザの協力を得られずに、新バージョンは購入したものの導入できない、といった事態が発生する可能性がある。そのため、情報セキュリティの予算としてどの範囲を認識しているのかを確認した。

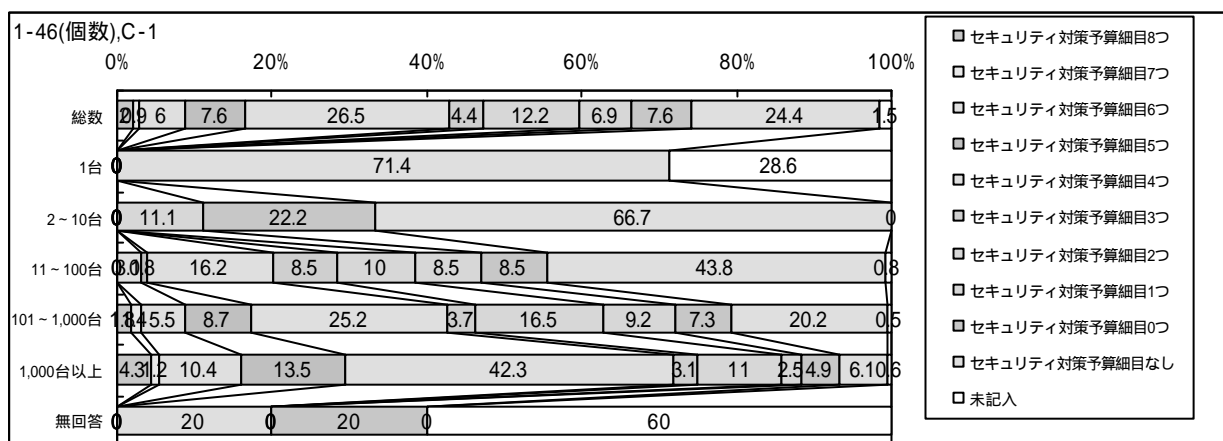


図 5-41 1-46×C-1 情報セキュリティ関連予算勘定科目数 (PC台数別内訳)

図 5-41 の横棒の内訳は、問 1-46 で情報セキュリティ関連の予算として計上している勘定科目数を表す。つまり 勘定科目数が多いほど情報セキュリティ対策の具体的な内容を把握し、リソースを確保していると見なすことが可能である。

上記の予測どおり 保有 PC 台数が増加するにつれて、情報セキュリティ対策予算項目の数が増加した。

情報セキュリティ対策の人材確保 図 5-12、5-38、5-39、参照

2.9. 技術的な情報セキュリティの確保状況 情報セキュリティ技術の導入状況

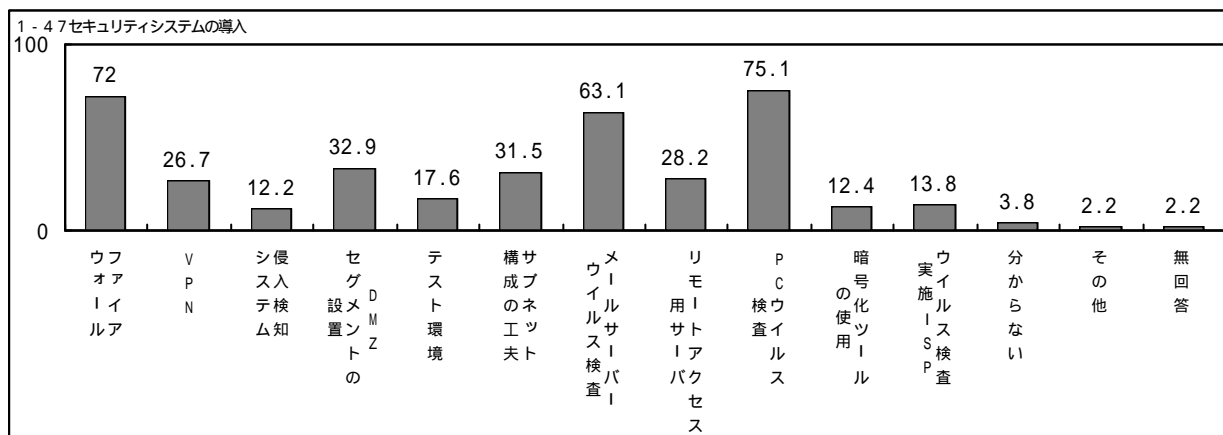


図 5-42 1-47 情報セキュリティへの体系的対策

情報セキュリティを確保するために導入している情報システム関連技術を確認したところ、「ファイアウォール」が72%、「PC ウィルス検査」が75.1%、「メールサーバーウイルス検査」が63.1%と過半数の企業で導入済であることが判明した。しかし、テスト環境をもつ企業の割合が低かった。

情報セキュリティポリシーでコンピュータウイルス対策が制定されている場合、実際にアンチウイルスソフトを全クライアントPCで導入しているかを確認し、ポリシー上での規定と現状の乖離を確認した。

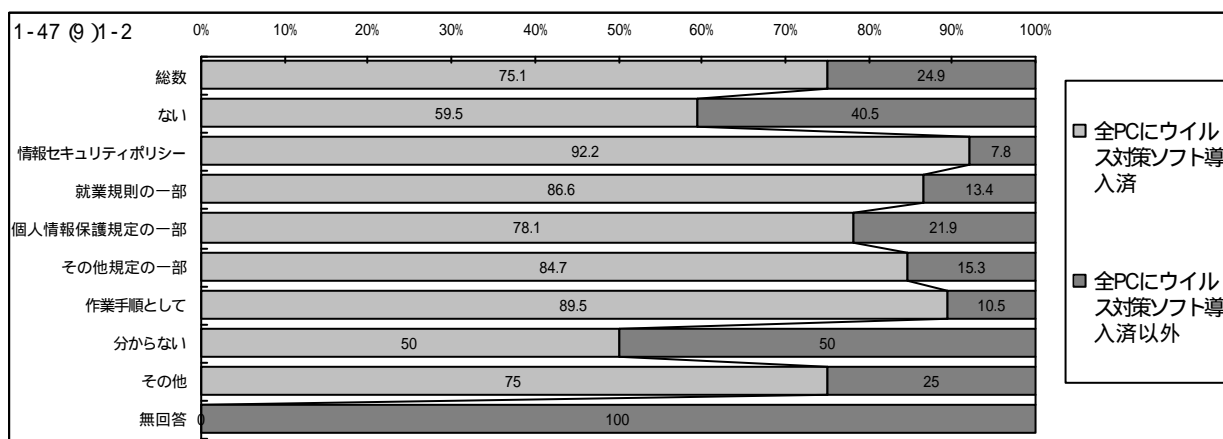


図 5-43 (1-47(9))1-2 アンチウイルスソフトの導入状況と関連ポリシーの有無

情報セキュリティポリシーが「ない」と回答した企業は「全PCにウイルス対策ソフト導入済」と回答した割合が59.5%だった。一方で、「情報セキュリティポリシー」を持つ企業は、「全PCにウイルス対策ソフト導入済」と回答した割合が92.2%であった。

3. 情報セキュリティ対策（インシデント対策）の問題点把握

3.1. 情報セキュリティ問題による被害状況

図 5-44 は情報セキュリティ問題（情報セキュリティ関連の事件や事故、インシデント）の発生状況を表している。発生した問題の内訳別に、情報セキュリティ問題の発生企業数の合計を縦棒グラフで、発生件数の合計を折線グラフ（ ）で表示し、対処に要した人日を折線グラフ（ ）で表示した。回答企業数の合計（縦棒）の目盛りが表右縦、発生件数（ ）と対処人日（ ）の目盛りは表左縦である。

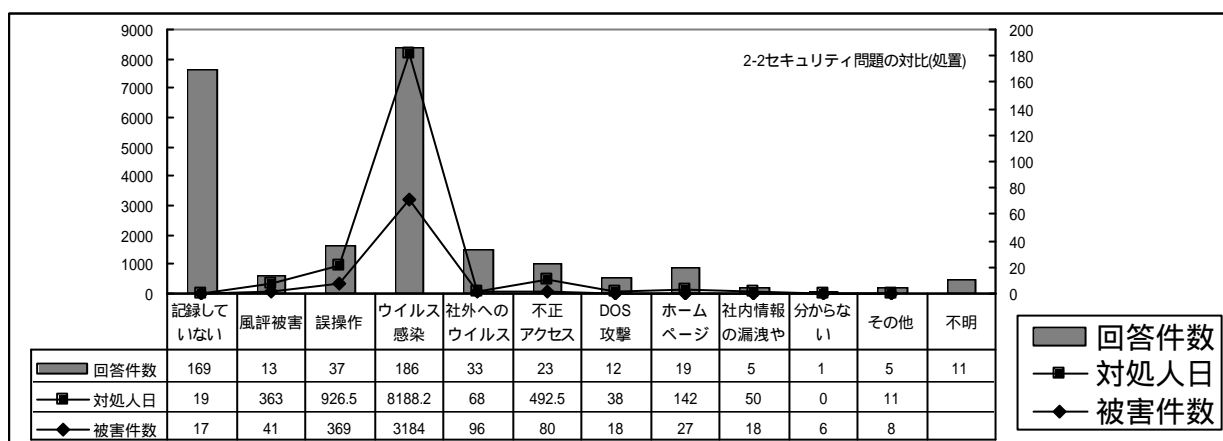


図 5-44 2-2 情報セキュリティ問題の被害状況

ウイルス感染の被害件数、被害企業数がその他の被害に比較して高かった。次いで誤動作による被害が続いている。対処人日÷被害件数で1件あたりの平均対処人日が見える。「社外へのウイルス発信」における対処では、自社の被害の把握や情報資産の復旧以外にも、被害者への説明責任等が含まれる。しかし、1件あたりの対処人日が0.7人日程度と他の情報セキュリティ問題への1件あたりの対処人日と比較して低いことが分かる。

情報セキュリティ事故や事件に適切に対処するためには現状を理解するための情報収集が重要である。しかし、情報セキュリティ問題の被害状況を記録していない企業が169社あった。

3.2. 情報セキュリティ問題の原因

情報セキュリティ問題が発生する原因は多様である。適切な情報セキュリティ対策を導入することで、予防可能な問題もあれば、予測が難しい問題もある。各企業では、情報セキュリティ問題の発生原因をどのように認識しているのかを確認した。

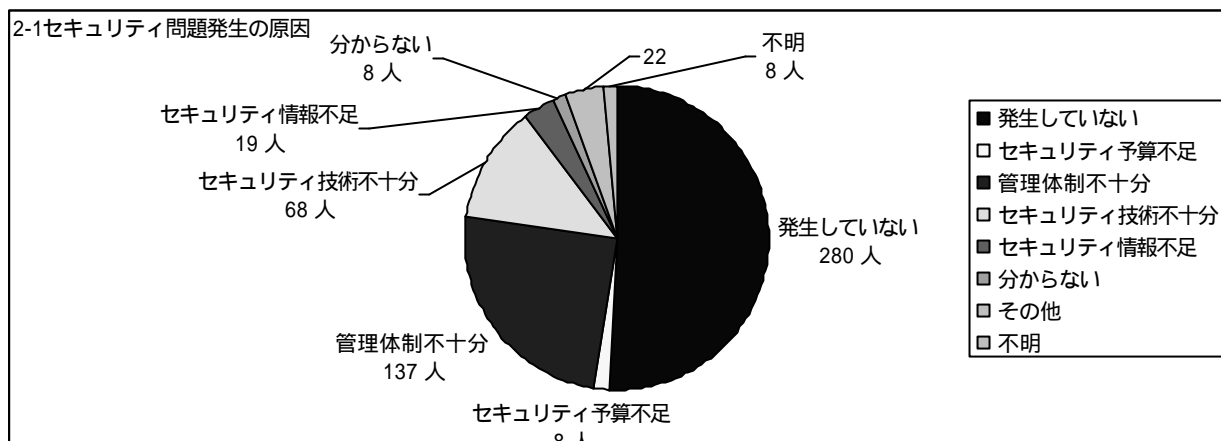


図 5-45 2-1 情報セキュリティ問題の発生原因

情報セキュリティ問題は「発生していない」との回答が約 51% (280 人) を占めた。しかし、図 5-44 で明らかになったように、情報セキュリティ問題の被害状況を記録していない企業が約 31% (169 人) と多かった。そのため、実際には発生している情報セキュリティ問題を把握していない企業が相当数に上ると推察できる。

情報セキュリティ問題が発生した原因として最も多かったのが情報セキュリティに対する「管理体制が不十分」であった、という理由であり全体の約 25% (137 人) を占めた。

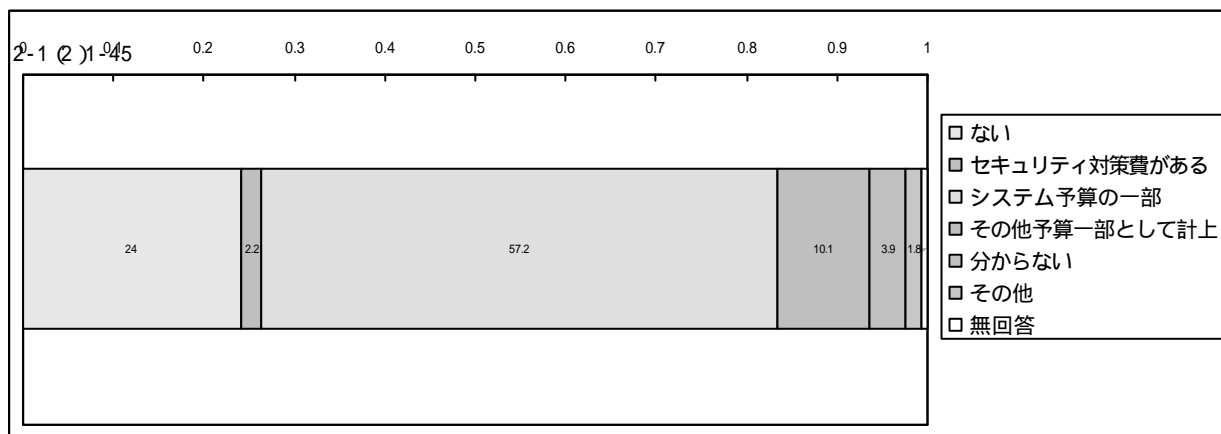


図 5-46 Q-1(2) X1-45) セキュリティ関連予算有無と問題発生原因の関係

情報セキュリティ問題が予算不足で発生したと考えている企業の、情報セキュリティ関連予算有無の内訳を確認した。情報セキュリティ問題が、予算不足のために発生したと回答した企業の多くが、情報システム予算の一部として情報セキュリティ対策予算を獲得していることが分かる。また、情報セキュリティ対策予算がないと回答した企業も多いことが分かる。

3.3. 情報セキュリティ問題に関する対応体制の整備状況

情報セキュリティ問題からの復旧作業の遂行

情報セキュリティ問題が発生する可能性を完全になくすことはできない。そのため、業務継続計画を制定し、問題が発生した場合には効率的かつ安全に情報セキュリティ問題からの復旧作業を遂行する必要がある。そのため、情報セキュリティ問題が発生した場合の復旧作業内容について確認をした。

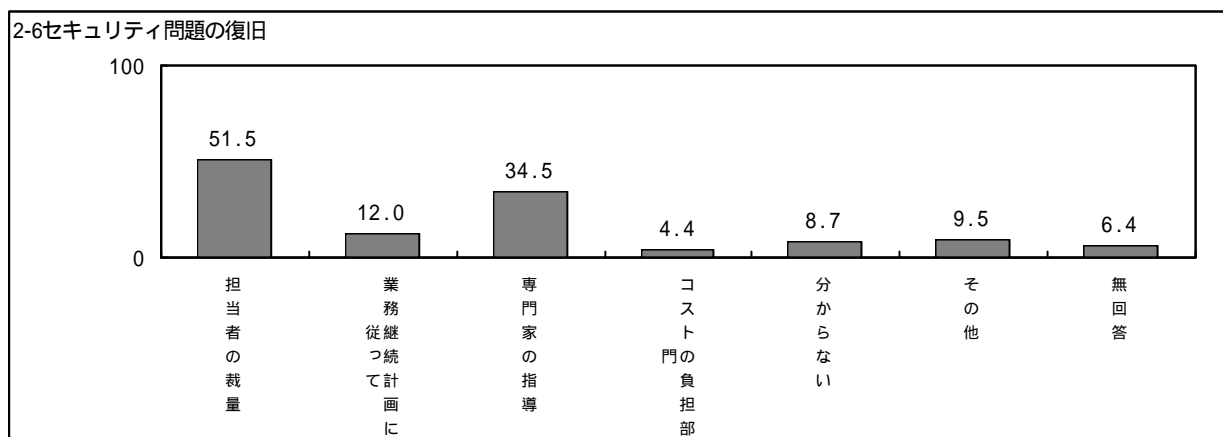


図 5-47 2-6 情報セキュリティ問題からの復旧作業

情報セキュリティ問題が発生した場合の対処方法として最も多かった回答は「担当者の裁量」で、51.5%であった。「専門家の指導」の下で対処を行うと回答した企業は34.5%であった。

情報セキュリティ問題に対処するためには、情報セキュリティ技術のみならず法務知識、広報等幅広い知識が必要である。問題に対して正しい対応ができない場合、2次被害として風評被害を被ったり、後日再び外部から情報システムに攻撃を受ける可能性がある。そのため、予め業務継続計画を制定し計画に従って対処する、または専門家の指導の下で対処を行う必要がある。

情報セキュリティ問題の認識方法

情報セキュリティ問題が発生した場合には、発生と同時に問題を検知し最も適切な方法で対処する必要がある。そのため、発生する可能性のある問題を洗い出し、発生した場合の対処手順や連絡方法を予め制定しておくことが重要である。

情報セキュリティ問題が発生した場合、問題の発生を検知し、被害状況を把握する等の対処が必要になる。しかし、情報セキュリティ問題を検知する体制がない企業が多いのではないかと考えられた。そのため、企業規模別に情報セキュリティ問題発生時の問題の検知(認識)方法を確認した。

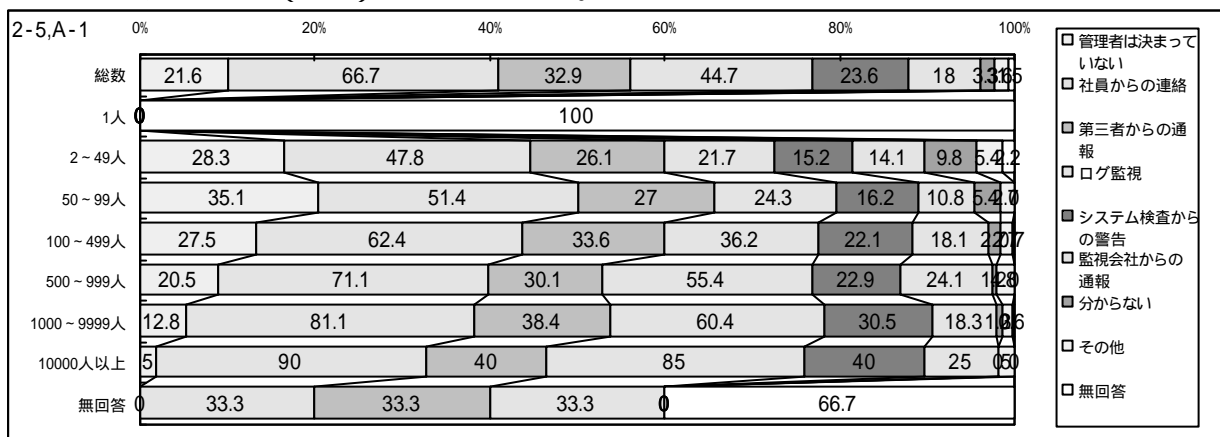


図 5-48 2-5 x A-1 情報セキュリティ問題の認識方法 (企業規模別内訳)

図 5-48 のとおり、従業員数が増加するにつれて、情報セキュリティ問題の認識方法として「ログ監視」や「システム検査からの警告」と回答した企業の割合が増加した。しかし、従業員数が増加するにつれて、「分からない」との回答の割合も増加している。

定期的にサーバのログ解析を行い、不正アクセスの有無を調査している企業では、システム検査や目視等によるログ解析による情報セキュリティ問題の発見件数が多いのではないかと考えた。そのため、定期的にアクセスログの解析を実施している企業と未実施の企業の情報セキュリティ問題の発見方法の内訳を確認することにした。

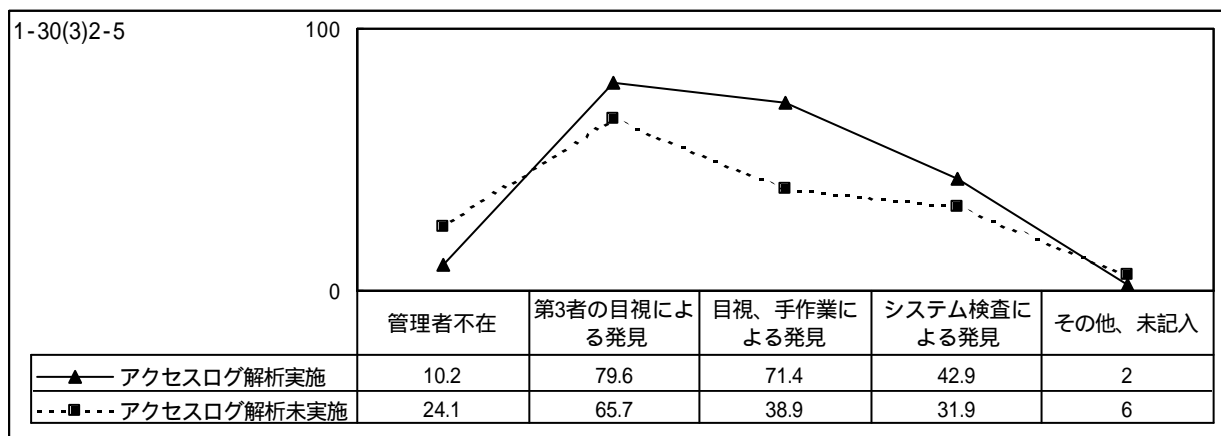


図 5-49 (1-30(3))2-5 不正アクセスのログ解析有無別情報セキュリティ問題の認知方法

図 5-49 の通り、定期的にアクセスログを解析している企業としていない企業の間では、全体的にアクセスログを解析している企業の発見平均数が高いことが分かる。しかし、両者の間に情報セキュリティ問題の発生認識方法に大きな差異は見られなかった。これは、情報システムを導入しただけでは情報セキュリティ管理として不十分であり、システムを有効に活用するための体制が必要であると考えられるだろう。

3.4. 情報セキュリティ問題に関する対応技術の習熟度

情報セキュリティ問題に対応する人材の有無

情報セキュリティ問題に適切に対処するためには、情報システム技術を有し、情報資産の重要性を理解して被害と影響を適切に切り分けることのできる人材が必要である。また、社内外にどのようにして問題を告知するのか(または告知しないのか)を考え、適切な処置を行う必要がある。これらの対処が可能な人材は少なく、情報セキュリティ問題の発生後に情報セキュリティの専門企業に対処を依頼する企業もある。

後述する第4節の通り、情報セキュリティ管理において現在民間企業が最も望んでいる対策は、情報セキュリティ教育や情報セキュリティ関連コンテンツの提供や啓発活動等、人材育成や教育が中心であった。そのため、どのような業界や企業規模等の企業で最も人材が不足しているのかを把握するため、各企業の人材の有無を、企業規模別や情報セキュリティポリシーの整備状況別等に分けて確認した。

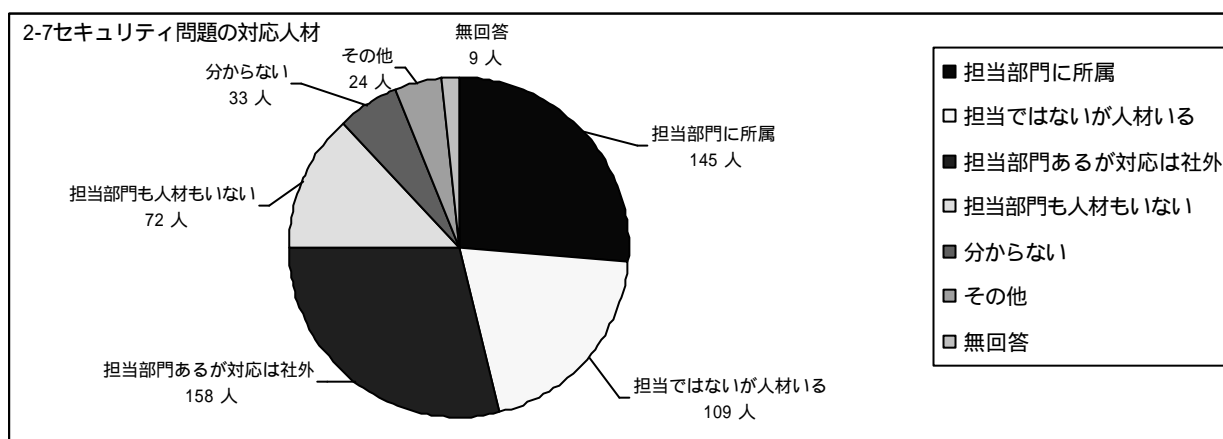


図 5-50 2-7 情報セキュリティ問題への対応可能な人材の有無

情報セキュリティ問題が発生した場合の対応としては、情報セキュリティの「担当部門あるが対応は社外」に依頼すると回答した企業が約 29% (158 人) と最も多かった。情報セキュリティの担当部門のリソースが限られている場合は、社内の情報セキュリティの担当部門は、日常的な運用や情報セキュリティ教育を主に担当し、情報セキュリティ問題が発生した場合にはより深い知識を有する専門家に依頼する、という体制は、社内の限られたリソースを有効に活用するという意味からは好ましい対応だと言えるだろう。

情報セキュリティ問題に対処可能な人材の有無を、売上高別に見ると図 5-51 のとおりだった。基本的に、企業規模(売上高)が大きくなるにつれて情報セキュリティ問題に対処可能な人材が「担当部門に所属」「担当ではないが人材いる」と回答した企業の割合が増加していることが分かる。

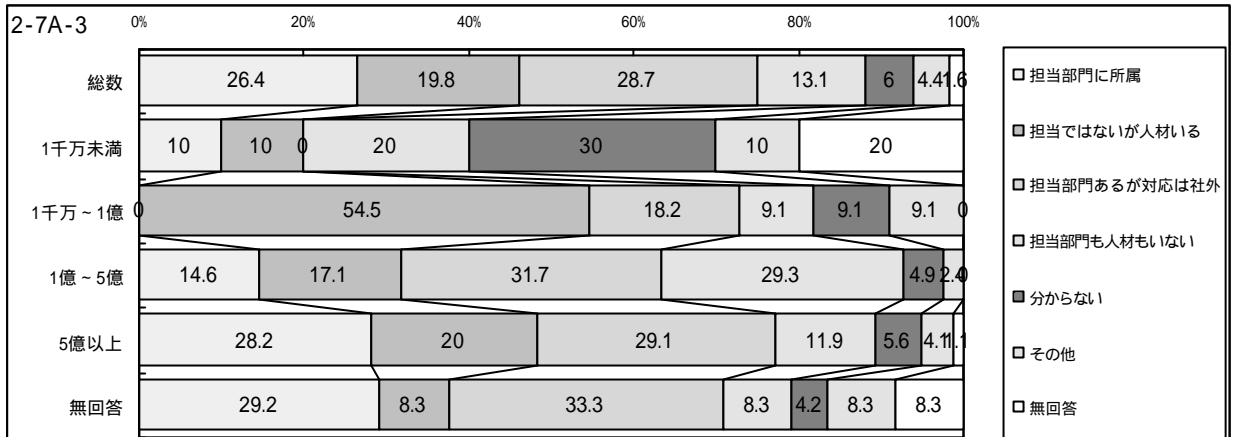


図 5-51 2-7×A-3 情報セキュリティ問題への対応可能な人材の有無 (企業規模別内訳)

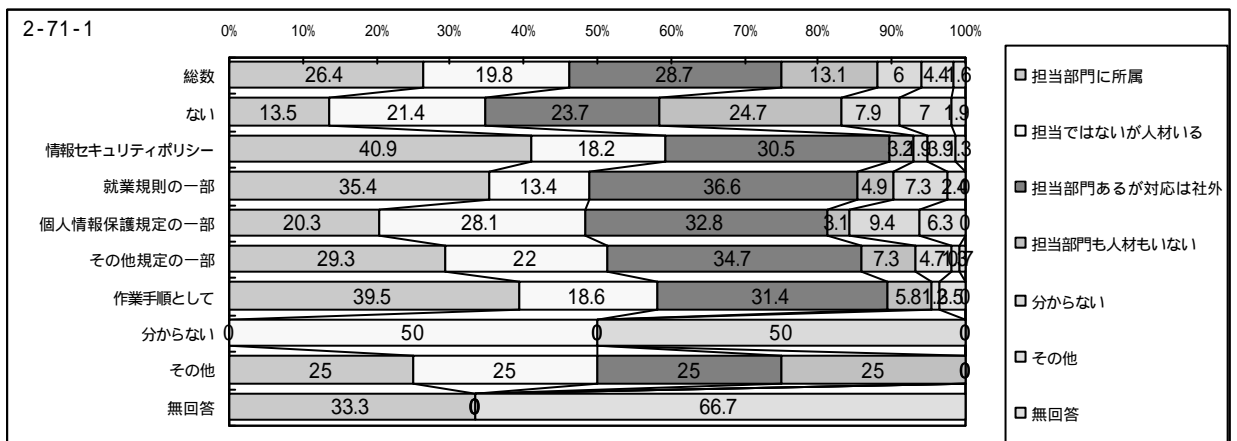


図 5-52 2-7×1-1 情報セキュリティ問題への対応可能な人材の有無 (ポリシー整備状況別内訳)

情報セキュリティ問題に対処可能な人材の有無を、情報セキュリティ関連規定の整備状況別に見ると図 5-52 のとおりだった。「情報セキュリティポリシー」や「作業手順」として「情報セキュリティ関連の規定を持つ企業では、情報セキュリティ問題に対処可能な人材が「担当部門に所属」している割合が高かった。これは、「情報セキュリティポリシー」や「作業手順」の整備過程で自社に対処する問題の範囲まで定めた上で人材を該部署に配属したためと考えられる。

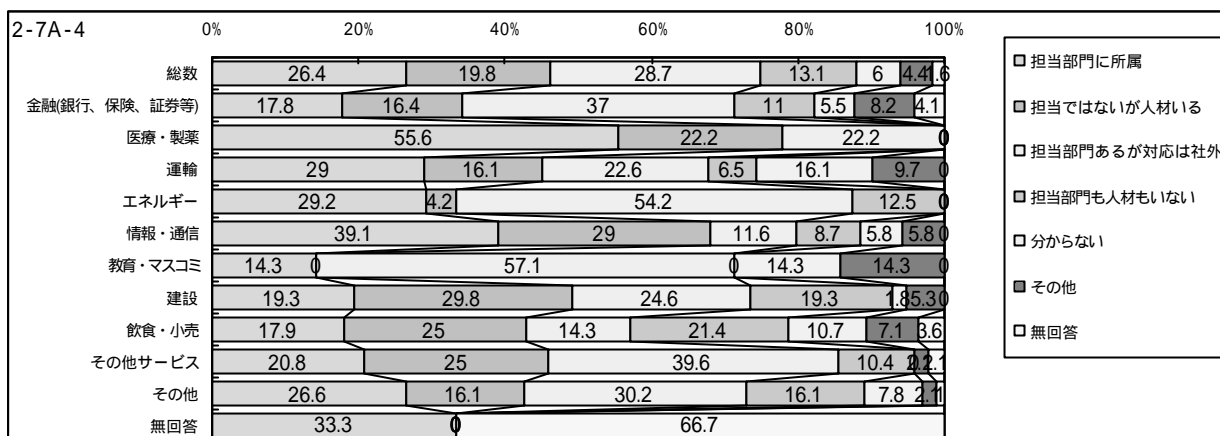


図 5-53 2-7×A-4 情報セキュリティ問題への対応可能な人材の有無 (業種別内訳)

情報セキュリティ問題に対処可能な人材の有無を、業種別に見ると図 5-52 のとおりだった。情報セキュリティ問題に対処可能な人材が「担当部門に所属」していると回答した割合が高い業種は、医療・製薬 (55.6%) と情報・通信 (39.1%) であった。

3.5. 情報セキュリティ問題発生時のアカウントビリティの確保状況

情報セキュリティ問題の社内告知

情報セキュリティ問題が発生した場合には、その影響と被害の範囲を確認し関係者各位に連絡をする必要がある。また、身近で問題が発生した場合には普段よりもリスク意識が高まっており、情報セキュリティに関する社内教育の好機である。そのため、各企業が説明責任、および社員教育の一環としてどのようにして情報セキュリティ問題を告知しているかを確認した。

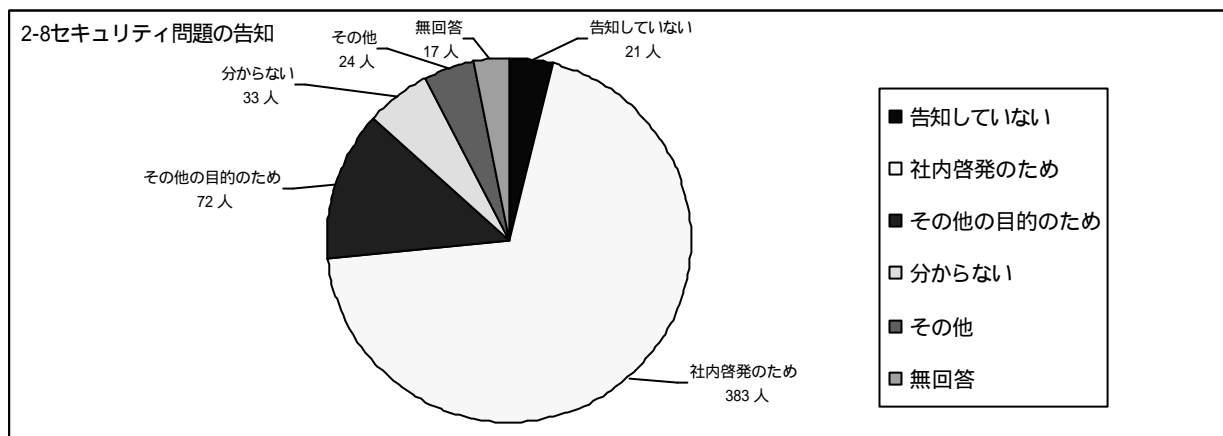


図 5-54 2-8 情報セキュリティ問題の社内告知

「社内啓発のため」に情報セキュリティ問題が発生したということ社内を告知している企業が全体の約70% (383人)であった。情報セキュリティ問題の発生を社内を告知していない企業は約4% (21人)であった。

図 5-54 の企業規模別内訳は図 5-55 のとおりだった。

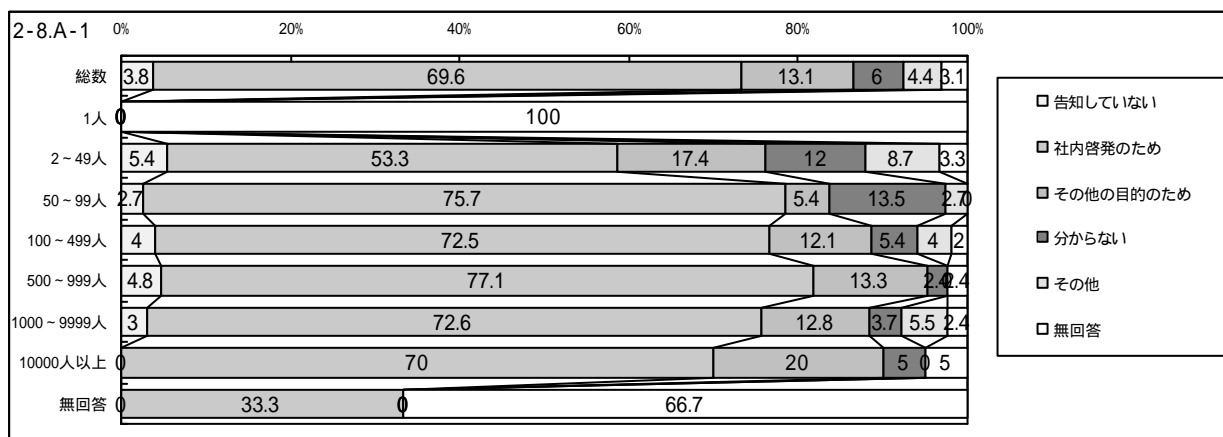


図 5-55 2-8×A-1 情報セキュリティ問題の社内告知 (企業規模別内訳)

従業員数が 50 人以上の回答を対象とした場合⁹、1 万人以上の企業で社内啓発以外の目的で社内告知をしている、と回答した割合が多かった。情報セキュリティ問題を社内で告知する目的としては、情報セキュリティに対する啓発のほかに、社外に対する説明責任、被害の拡大防止等が考えられる。

特に大企業では、コンピュータウイルスの感染等を発見した場合に即時に全従業員に告知することで、警戒が高まり被害の拡大を防止するという意義が大きいと考えられる等の効果が考えられるため、「その他の目的のため社内告知をする」と回答した企業が多かったのではないかと推察できる。

⁹ 従業員数 50 人未満の企業は 94 社である。母集団に比較して小数であるため、比較の対象から外した。

情報セキュリティ問題の社外告知

情報セキュリティ問題が発生した場合には、その影響と被害の範囲を確認し関係者各位に連絡をする必要がある。しかし、こうした問題の発生を社外に告知すること自体にためらいを感じる企業も少なくないだろう。しかし、情報セキュリティ問題はインターネットを通して一瞬のうちに全世界に知られ、電子掲示板に書き込まれる等、2次被害としての風評被害を引き起こすことがある。このような風評被害を受けないためにも、適切な方法で社外告知を行う必要がある。

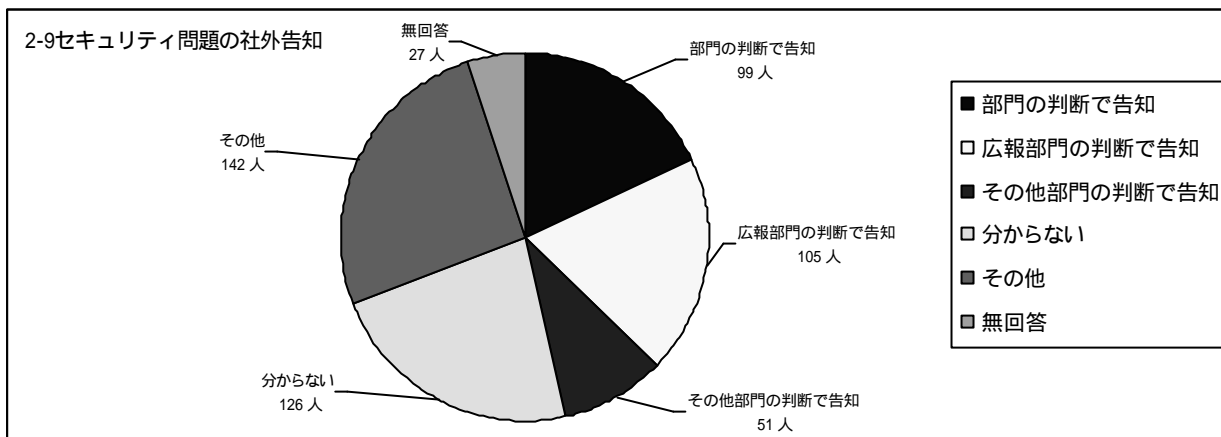


図 5-56 2-9 情報セキュリティ問題の社外告知

情報セキュリティ問題が発生した場合の社外告知の方法が「分からない」との回答が全体の約 23% (126 人)であった。また、その他が約 26% (142 人)であった。このことから、問題の発生の際に対処方法を検討し、実施している状況が推察できる。情報セキュリティ問題への対応は、発生毎に考慮すべき点もある。しかし、社外にウイルスを発信してしまったことが判明した場合の対処手順や、ホームページが改竄された場合の対処方法等、事前に対処を定めることで迅速な対応が可能になり、体外的な信頼性を保つことが可能となる。そのためにも、業務継続計画を定め、その中で責任体制や社内外を含めた説明責任について定めることが大切である。

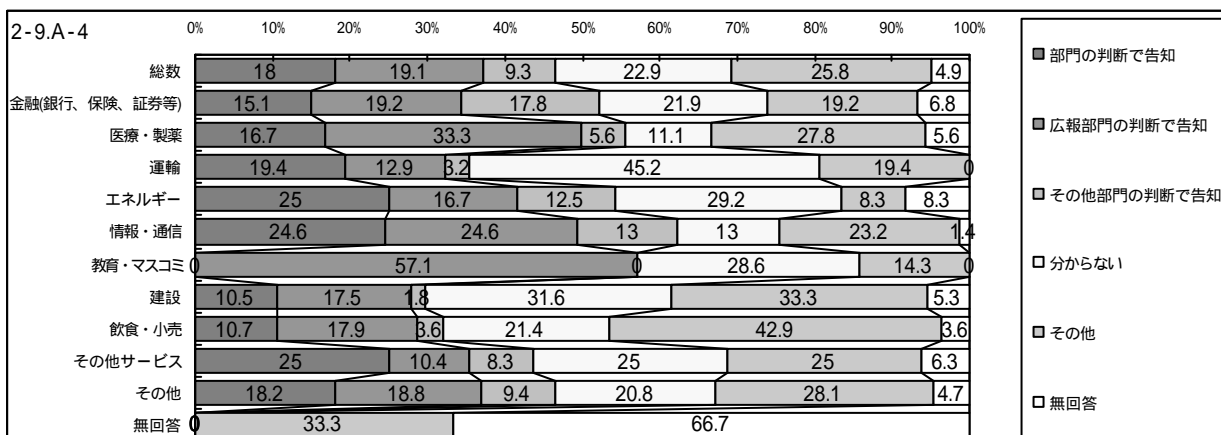


図 5-57 2-9×A-4 情報セキュリティ問題の社外告知 (業種別内訳)

業種別に内訳を見ると図 5-57 のとおりであった。情報セキュリティ問題が発生した場合の社外告知方法が「分からない」と回答した割合が高い業界は運輸、建設、エネルギー、教育業界の4業界であった。

情報セキュリティ問題復旧後の安全性確保

例えば会社のホームページを書き換えられた場合、書き換えられたホームページを単純に元に戻すだけでなく、余計なプログラムが書き込まれていないか、バックドアが設置されていないか等のシステムのテストを実施する必要がある。また、書き換えられた原因を突き止め、システムの不具合や問題があった場合には適切なパッチを当てる等の処置を行う必要がある。しかし、一度攻撃を受けたシステムは次回以降も攻撃の対象となりやすいため、情報セキュリティの専門家によるシステムのテスト(ペネトレーションテスト:PT)や監査を受けてから、本番環境に移行しシステムを公開することが望ましい。そのため、情報セキュリティ問題を復旧する際の手順やテストについて確認した。

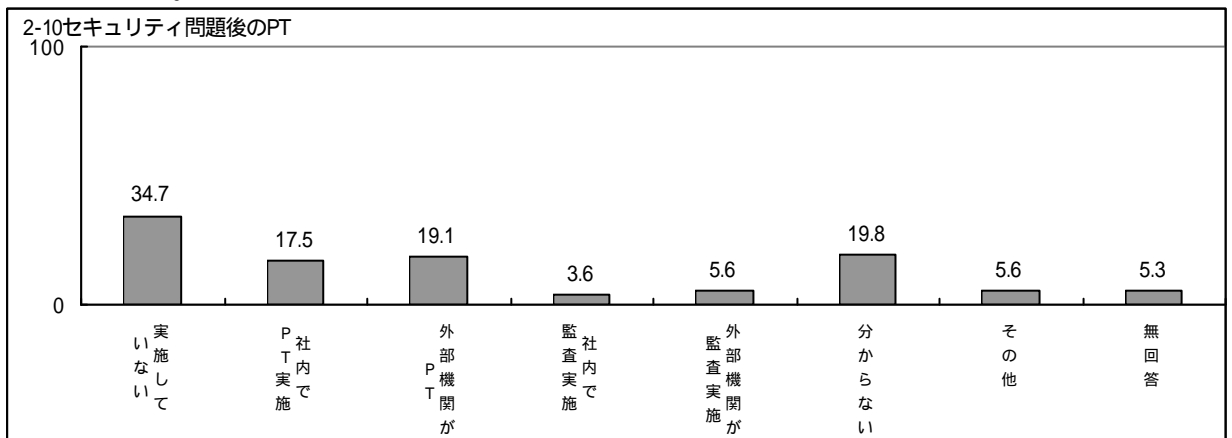


図 5-58 2-10 情報セキュリティ問題発生後の PT テスト実施有無

情報セキュリティ問題を復旧した後で、システム監査やペネトレーションテストを実施していない企業が全体の 34.7% で最も多かった。「社内で PT 実施」「外部機関が PT」と回答した企業はそれぞれ少なく、「社内で監査実施」「外部機関が監査実施」と回答した企業はそれぞれ 3.6%、5.6% とさらに少数だった。

本来はペネトレーションテストでセキュリティホールを確認し、システム監査で情報セキュリティに対する組織的なマネジメント体制を確認する必要があるが、ペネトレーションテストやシステム監査を実施する企業は少ないことが判明した。

図 5-58 の情報セキュリティポリシーの有無別内訳は図 5-59 のとおりだった。

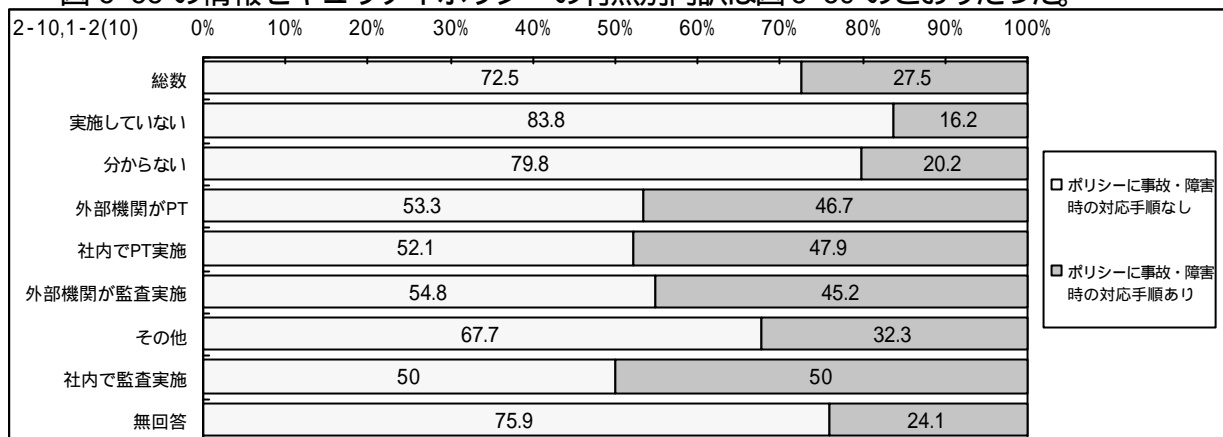


図 5-59 Q-10 X1-2(10) 情報セキュリティ対応に関するポリシーの有無と現状の関係

図 5-59 の横棒の内訳は、情報セキュリティ問題が発生した場合の対応手順を規定として定めている企業と定めていない企業である。

ペネトレーションテストやシステム監査を「実施していない」「分からない」と回答した企業とその他を比較すると、「情報セキュリティポリシーに事故・障害発生時の対応手順がない」割合が高いことが分かる。

4. 情報セキュリティマネジメント 対策の改善方法の検討

4.1. 今後の情報セキュリティ対策の整備計画 (自社整備、アウトソーシング)

情報セキュリティ対策は、1企業が自社だけで実行することは難しい。情報セキュリティ関連の認証の取得を推奨したり、情報セキュリティ問題の加害者に対する罰則を強化するためには、公共団体の主導が必要になる。

自社で発生した情報セキュリティ問題の発生理由と被害状況を公開することで、他社が被害を受けることを防げる可能性が高い。しかし、こうした情報を収集し公開する団体は、企業の匿名性を保持するためには利益団体ではないことが望ましいだろう。

また、情報セキュリティの確保にはコストがかかるため1社では対策に限界があると考えている企業や、自社には情報セキュリティの技術者が不足しているために外部の協力が必要であると考えている企業等もあるだろう。

そのため、情報セキュリティを確保するにあたって、自社で整備可能であると認識している範囲と、外部の協力が必要であると認識している範囲の確認を行った。

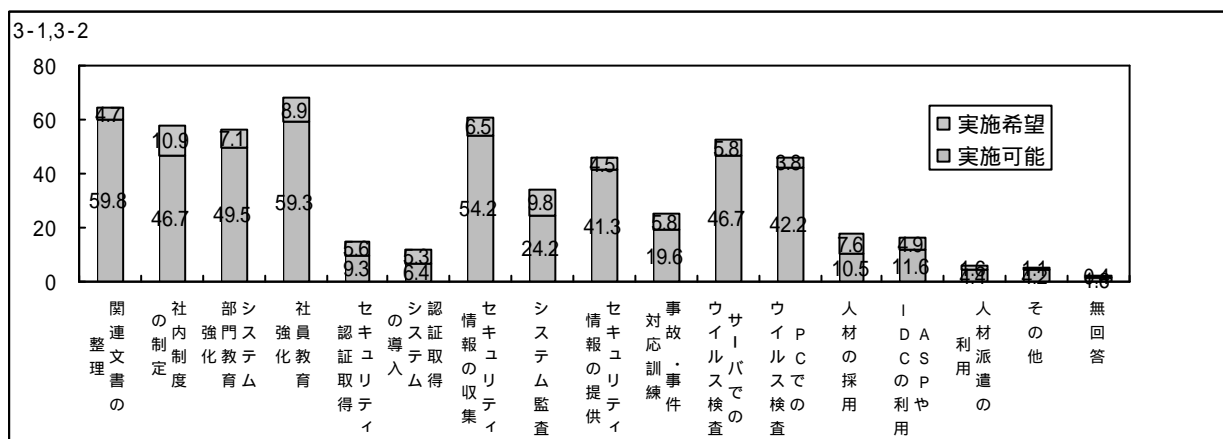


図 5-60 3-1+3-2 情報セキュリティ対策の実施希望と自社での実現可能範囲

図 5-60 の各縦棒の高さは、情報セキュリティ対策として実施を希望している企業数を表す。この縦棒の内訳は、濃い斜線が自社で実施可能であると考えている企業数である。つまり、薄い斜線は「自社で実施することは不可能、または難しいと考えている企業数」を表す。

情報セキュリティを確保するための対策としては、「社員教育の強化」「関連文書の整備」「セキュリティ情報の収集」の実施が望ましいと回答した企業が多かった。この3対策はその他の対策と比較すると、自社で実施可能であると考えている企業の割合が高かった。

自社での実施が難しいと考える企業の割合が高い対策は、「システム監査」「セキュリティ関連の認証取得」「人材の採用」であった。

4.2. 公共団体への期待

情報セキュリティマネジメントにおいて公共団体に期待する役割

情報セキュリティ対策を継続的な活動として捉え、官民が一体となった情報セキュリティの向上を目指すためにはどのような施策が必要であるのか、また望まれているのかといった意識についての情報を収集した。

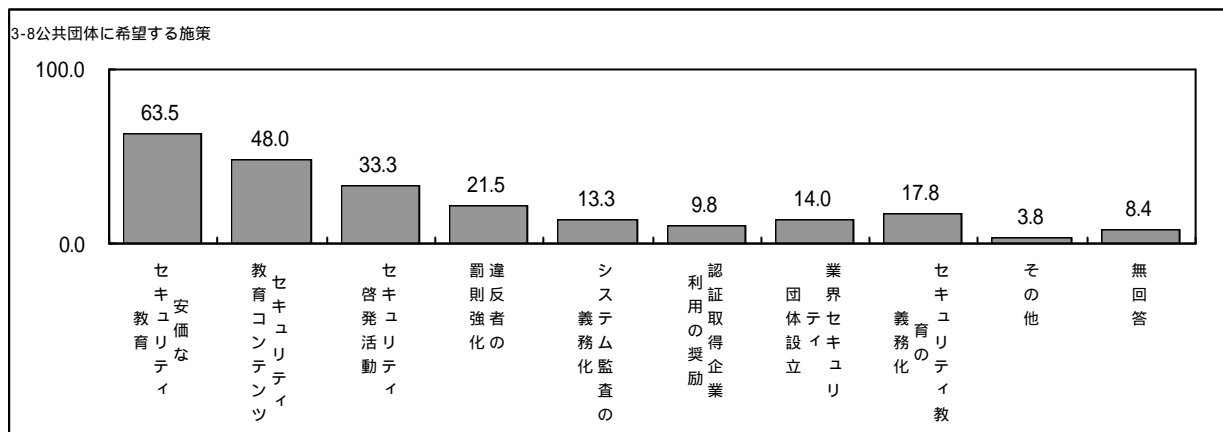


図 5-61 3-8 公共団体に希望する情報セキュリティ対策

情報セキュリティ対策として、公共団体に求める施策のトップ3は「安価なセキュリティ教育の提供」(63.5%)、「セキュリティ教育コンテンツ」の提供(48.0%)、「セキュリティ啓発活動」(33.3%)であった。公共団体に求める役割としては、情報セキュリティ教育に関する要望が強いといえる。

企業規模別に、公共団体に希望する情報セキュリティ対策に差異がないか確認したところ、図 5-62 のとおりであった。

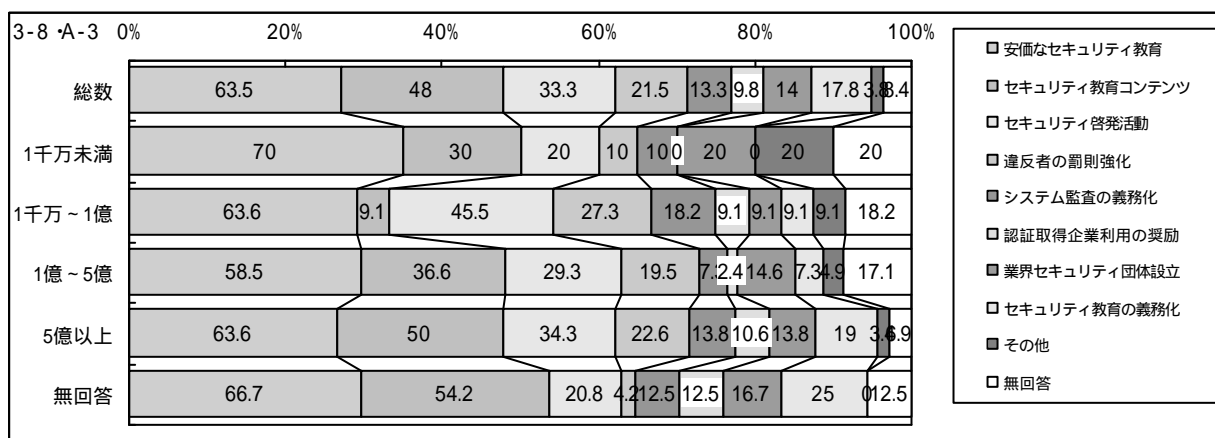


図 5-62 3-8×A-3 公共団体に希望する情報セキュリティ対策 (企業規模別内訳)

企業規模(売上)別に、公共団体に希望する情報セキュリティ対策を比較したところ、売上高1千万未満の企業が公共団体に求める対策としては「安価なセキュリティ教育の提供」が最も多かった。売上高1億以上の企業でも、「安価なセキュリティ教育の提

供」を望む割合が最も高かった。しかし、売上1億未満の企業と比較すると「セキュリティ教育コンテンツの提供」と回答した割合がやや高かった。

そのため、中小企業に対しては、情報セキュリティ教育研修の実施を行い、中堅企業や大企業に対しては情報セキュリティ教育研修と同時に情報セキュリティ関連の教育コンテンツを提供するという方向の支援が望まれていると言えるだろう。

業種によっても、取り扱う情報資産の機密性や可用性に差異があるため、公共団体に求める協力内容が異なる可能性もある。そのため、業種別の内訳も確認した。

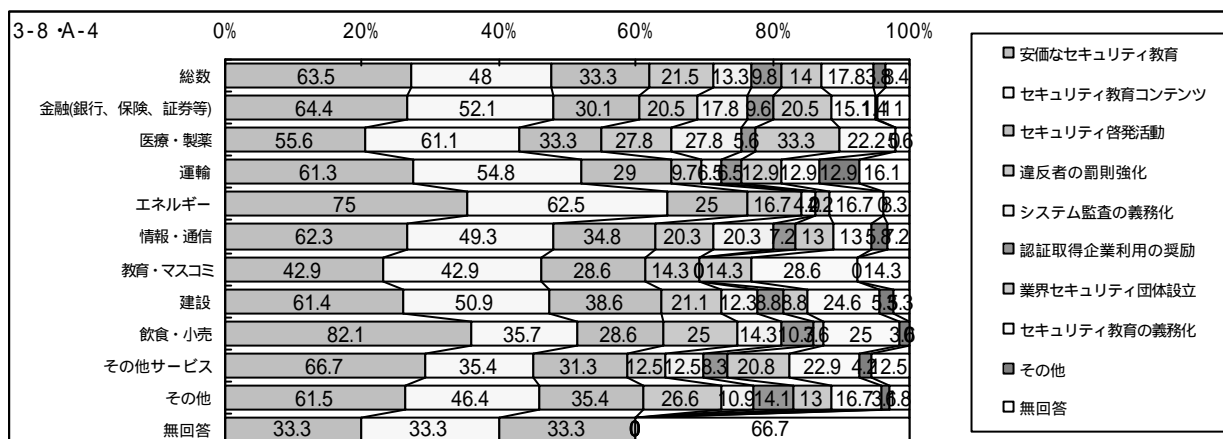


図 5-63 3-8×A-4 公共団体に希望する情報セキュリティ対策 (業種別内訳)

飲食・小売、エネルギー業界で「安価なセキュリティ教育の提供」と回答した割合が高かった。また、金融、建設、情報・通信、医療・製薬業界では、他業種と比較して「認証取得企業利用の奨励」と回答した割合が高かった。

情報セキュリティの実態調査
- 2001 年 調査報告書 -

13 情経第 1112 号

情報処理振興事業協会
セキュリティセンター
禁無断転載

本報告書は、公募により採択された KPMG ビジネスアシュアランス株式会社に委託して実施した調査の結果をまとめたものである。