企業等における脆弱性対策に関する
実態調査報告書

2011 年 2 月

独立行政法人 情報処理推進機構
セキュリティセンター

目　次

1. 調査概要

1.1. 調査目的

国内の企業等の組織においては、予算や体制、スキル等の制約もあり、十分な脆弱性対策が適用されているとは限らない。そこで、企業等の脆弱性対策の現状や課題に関するアンケート調査を実施のうえ、実態を把握し、課題を分析する。

本調査においては以下の目的を設定している。

- 国内における企業等の組織における脆弱性対策の状況に係る実態の定量的把握
- 脆弱性対策の普及・推進にあたっての課題抽出に関する分析

1.2. 調査対象

■プレヒアリング

企業における脆弱性対策の実態に即した質問を行うため、本格的なアンケートに先立ち、以下の要領で企業等のセキュリティの実態に詳しい有識者にプレヒアリングを行い、この結果を本調査のアンケートの設問および仮説に反映した。

［調査方法］ 訪問ヒアリング
［調査対象］ 国内の大企業、中小企業、政府機関、地方公共団体の情報セキュリティ担当者。各 1 件。

■アンケート調査

回収の確実性を重視し、企業モニターを対象としたウェブ・アンケート調査を行った。調査精度を向上させるため、調査モニターの IT 担当者に対してプレ調査を行い、回答者の中からセキュリティ担当者を抽出した上で本調査にあたっている。

本調査は全国の企業等のセキュリティ担当者 310 件を調査対象として実施した。

［調査方法］ ウェブ・アンケート調査（企業モニター）
［調査対象］ 国内企業等のセキュリティ担当者
［有効回収数］310 件

1.3.調査実施期間

2010 年 7 月

1.4. 調査項目

調査の主な設問項目は以下の通りである。

＜プレ調査の設問項目＞

（１）回答者の所属する企業等の基本属性

（２）担当する情報システムのオーナー

（３）情報セキュリティに係る業務への関与

（４）関与する情報システムの種別

（５）IPA の脆弱性関連事業に関する認知度

＜本調査の設問項目＞

（１）IT および情報セキュリティ対策全般の状況

（２）脆弱性とその対策に関する情報収集・分析の状況

（３）ウェブサイトの脆弱性対策に関する状況

（４）組織内向けシステムの脆弱性対策に関する状況

（５）クライアント PC の脆弱性対策に関する状況

（６）脆弱性対策に関する課題

＜企業モニター回答者の属性＞

（１）業種

（２）従業員数・職員数

1.5.調査結果概要

①脆弱性対策の整備状況に基づく分析

- 組織規模により脆弱性対策の取り組みに格差が見られた。大企業等は体制や手順を整え、WAF や統合管理ツール等も導入し、JVN 等の情報も有効に活用しているのに対し、中小企業等は被害経験が乏しく、対策の必要性を強く感じていないものと考えられる。
- ウェブサイトに対する脆弱性検査や脆弱性診断サービスは、大企業等で約 8 割、中小企業等でも約 4 割が実施しており、一般化しつつあるといえる。
- 組織内向けシステムに比べウェブサイトにおける脆弱性対策が遅れている傾向が見られた。これはウェブサイトについては現場主導の構築・運用がなされやすいため、組織的な脆弱性対策の意識付けが乏しいと推測される。
- WAF は、大企業等の約半分、中小企業等の約 1/4 が活用しており、ウェブサイトの脆弱性対策において重要な役割を担っていることがわかる。しかし、WAF を利用している組織の 1/3 が「ウェブアプリケーションの修正を行わない」と回答しており、根本的な対策がなされていない状況が伺える。
- クライアント PC の脆弱性対策において、統合管理ツールは大企業等の約 4 割が活用している一方、中小企業等の活用は 1 割に満たない。このことから、統合管理ツールは、規模の負担を軽減するツールとしてのポジションを確立していることが伺える。

②脆弱性対策の阻害要因

- 「増え続ける脆弱性に逐一対応するのは難しい」は「重要な課題とする」（34.8%）、「課題の一つである」（42.6%）と、最も重要かつ高い支持を集めた課題である。
- プレヒアリングにおいて指摘があった「事業を継続したいシステムのオーナー部門と脆弱性対策を行いたいセキュリティ担当者の対立」という仮説は、大企業等では「重要な課題である」（25.3%）、「課題のひとつである」（44.8%）との認識を示しており、検証できたと考えられる。ただし、中小企業等では、システム担当者（セキュリティ担当者）自身が直接管理しているケースが多いため、対立構造にならず「特に重要な課題ではない」が約 6 割という結果になったと考えられる。

③脆弱性対策の普及推進における課題

- 運用中のシステムの脆弱性対策を外部委託する場合、「契約には明記されていないが、事実上、委託費用に全て含まれている」との解釈を示す回答が高い割合で見られた。増加する脆弱性の状況を考慮すれば、委託先の負担はバランスを欠いたものになりかねない。今後、改善に向けた取り組みがなされることを期待する。
- ウェブサイトの脆弱性に気付くきっかけは、大企業等の 41.4%が「セキュリティ関連組織等から連絡を受けた」ことを挙げていること、また、大企業等の 33.3%、中小企業等の 18.2%が

脆弱性対策の判断時に「セキュリティ関連組織等が提供する情報」を参考にしていることから、情報セキュリティ早期警戒パートナーシップの取り組みが効果を挙げていることがわかる。ただし、情報セキュリティ早期警戒パートナーシップや脆弱性関連情報届出受付（IPA)、製品開発者調整（JPCERT/CC)、JVN 等の認知度や利用経験にはまだ向上の余地がある。特に、中小企業等への啓発が遅れている状況の改善が望まれる。

2. 調査分析の方針

2.1. 調査項目の設定

企業等において利用される情報システムへの脆弱性対策についての実態について、より詳細な把握を行うため、本調査では対象の情報システムを次の 3 つに大別して調査項目を設定した。

- ウェブサイト：組織がインターネットに公開し、主に組織外とのやり取りに用いる。ウェブサーバ、データベースサーバ等で構成されるもの。
- 組織内向けシステム：グループウェアサーバ、ファイルサーバ、ディレクトリサーバ、バックアップサーバ等のイントラネット上のシステム。クライアント PC は除く。
- クライアント PC：特に OS、ミドルウェア、アプリケーションソフトウェアなどのソフトウェアを調査対象とする。

2.2. 調査仮説

次の調査仮説を立てて調査にあたった。

仮説(1)：「既に脆弱性対策を進めている組織」「これから脆弱性対策を進める組織」の特徴

脆弱性対策の進展の度合いを、組織における脆弱性対策の整備状況に基づいて 2 グループに分類し、各グループの特徴の抽出により、脆弱性対策の普及推進における課題の明確化を狙う。仮説検討の作業の流れを下図に示す。

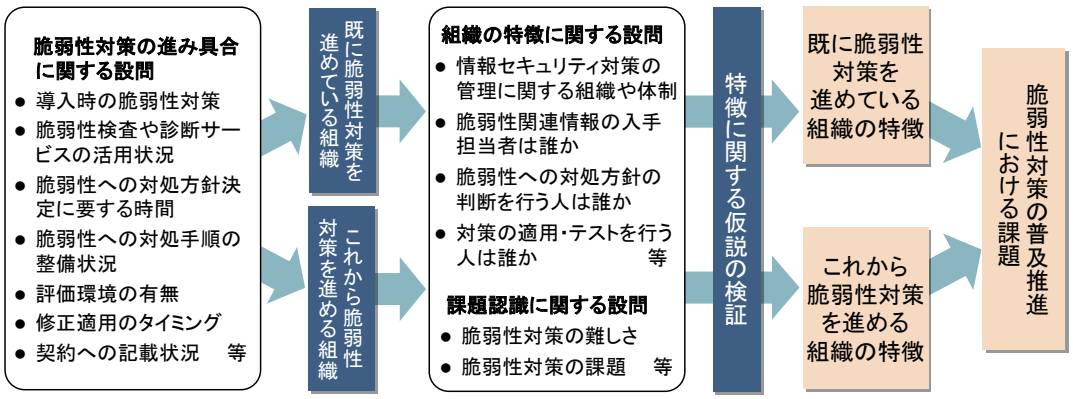

図 2.2-1　仮説(1) ― 検討の流れ

脆弱性対策の進展の度合いと特徴についての初期仮説を下表に示す。

表 2.2-2　仮説(1) ― 初期仮説

	開発・運用の体制	脆弱性対策の体制等	保守予算	脆弱性の緊急対処
既に脆弱性対策を進めている組織	外部リソースを有効活用している。	体制や責任範囲が整備されている	保守予算を確保している	柔軟に対応
これから脆弱性対策を進める組織	大半を内製している	要員確保が困難	保守予算確保が困難	硬直化した対応

仮説(2)：企業属性による分類、および、該当領域における脆弱性対策の阻害要因

「企業規模」と「IT 投資」を分類軸として調査対象の組織を 4 象限に大別し、各領域に属する組織において脆弱性対策を阻害する要因を次のように仮定した。

（阻害要因の例）

- システムオーナーの理解が乏しい
- アプリケーションに影響するためパッチを適用できない
- 関連情報が大量のため、負担が重い
- パッチ適用の判断が難しい
- 知識のあるシステム保守要員が不足
- システム保守予算が不足

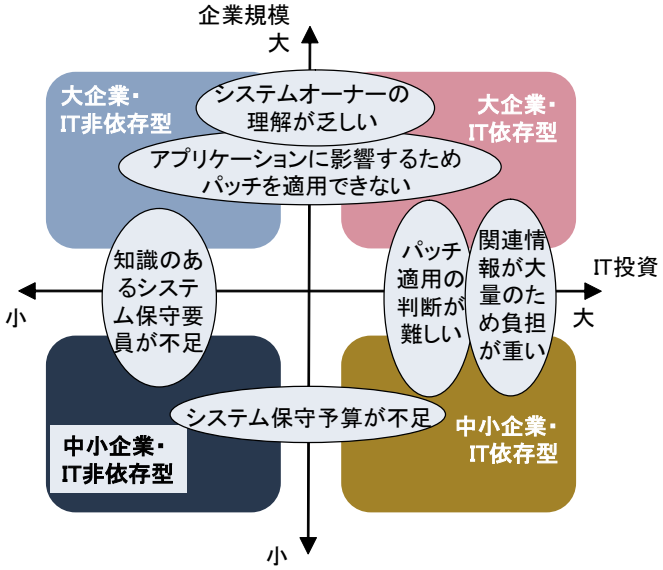

図 2.2-3　仮説(2) ― 分類軸および阻害要因

2.3.プレヒアリング

プレヒアリングでは仮説に基づいて作成したアンケート設問の原案を示し、それらの設問に関する実態について伺った。また、実態と乖離している等の理由で回答が困難な設問・選択肢についての指摘をいただいた。以下にヒアリングで得た主なコメントを示す。

■中小企業

[体制：予算]

・情報システムを専門とする部署は無く、情報セキュリティ関連の運用を総務部門内の少数名が担当している場合がある。

[活動]

・情報セキュリティ対策の外部委託のひとつとしてメールのホスティングサービスによるウイルス対策を行っている。
・脆弱性対策の情報収集はしていない。
・PC の脆弱性対策のアップデートは各ユーザに任せている。
・取引先から情報セキュリティ対策に関する調査（アンケート）の依頼を受けた経験がある。
・脆弱性対策、ウイルス対策といった基本的な事項について経験と知識が無くあまり実感がわかない。

[事故・事件]

・ウイルスによる実質的被害は社員の時間が拘束される程度である。

[その他（要望等）]

・脆弱性情報の流通に興味を持たせる方策としては、脆弱性関連情報から数クリックで修正プログラムが適用できるようになればよい。考えずにクリックしてパッチがあたる機構ならば普及するだろう。

■自治体

[体制・予算]

・情報セキュリティについては総務部門とオーナー部門の共同であたっている。
・脆弱性対策の予算は取っていない。定期的な保守委託の範囲内かどうかを委託先担当者と協議している。予算を事前確保できず、予定していた支出を取りやめて差し替える。

[活動]

・ファイアウォールやリモート監視といった外部のセキュリティサービスも利用している。
・脆弱性対策は日常業務として遂行しており、情報セキュリティ関連組織からの情報提供も受けている。
・ウェブサイトおよび組織内システムについての構築・保守運用の委託はセキュリティ対策・脆弱性対策を含んだ内容で行っている。ウェブサイトについて自治体自身ではコンテンツの管理のみを行っている。
・システムのオーナー部門のリーダーが脆弱性対応について判断を下している。
・委託先に脆弱性対策対応を依頼する手順やポリシーが整備されている。
・PC のセキュリティについては統合管理機能を導入済みであった。だが PC への脆弱性対策の配信は帯域を占有するため難しいとのことであった。代わりに手作業で 3 ヶ月程度かかっている。
・脆弱性対策のきっかけとしては、攻撃の流行に関する情報を元に動くことが多い。法改正や通達も大きな要因である。
・組織外のシステムと連携しているシステムもあり、一律の回答が難しい。

[事故・事件]

・脆弱性に関して外部の通報を受けて対応した経験があった。
・脆弱性が係る攻撃としてウェブサイトに DoS 攻撃を受けた経験があった。

・クライアント PC については関係組織の者が持ち込んだファイルからウイルス感染した経験があった。
[その他（要望等]]
・啓発資料には障害・実害の事例が多数掲載されていることが望ましい。理解しやすい図が欲しい。特に利便性とセキュリティのバランスについて理解を促す内容を期待している。

■大企業
[体制・予算]
・情報セキュリティにかける支出総額の IT 投資における率は非常に低い。
・脆弱性対策の費用負担については、ケースが多くあり一律には考えにくい。検査費用はコストが発生するので嫌がられる。
[活動]
・仮想化されたサーバの場合も考慮してサーバ数をカウントする必要がある。
・ウェブサイトを構築し公開するだけでなく公開された他社のウェブサービスを活用する場合がある。
・情報収集は、海外から攻撃を受けるので迅速に情報を得るために海外の情報源を中心に行っている。
・サイトを停止するかについては事業の判断が優先する。システム部門は停止を勧めるが事業としてどうしても止められない規模のものもある。
・脆弱性対策の整備状況については、粗い規定はあるが手順にはしていない。ケースが多くそれぞれ対応が異なるため扱いが難しい。現在は明文化はしていないが対応はできている。
・動作トラブルが生じた際に脆弱性に気付く場合もあるだろう。
・脅威について評価を自組織で行うことが重要である。
・脆弱性を修正できる事業者が少ない点が問題である。

■中央府省庁
[体制・予算]
・情報セキュリティ対策の費用については、まとめて支出はしていない。様々な案件にそれぞれ費用が含まれている。
・緊急に対応する必要が生じた脆弱性対策に費用がかかる場合、このための予算の事前確保は困難である。
[活動]
・システム管理の単位ごとに個別に脆弱性情報の収集にあたっているが、セキュリティ担当の収集した情報も含め、共有している。
・ウェブサイトの仕様書には脆弱性対策を盛り込んでいる。
・ウェブサイトのセキュリティ診断の頻度は年 1 回程度である。
・脆弱性対策の適用の判断にあたっては運用している部門と調整している。
・組織内向けシステムについての脆弱性対策の適用に関する判断は、セキュリティ担当とも調整の上、システムオーナーの責任者が行う。
・脆弱性対策に係る人材の育成は、脆弱性以外についての知識も必要となるため難しい。

これらの情報を元にして設問・選択肢に変更を加えた上でアンケートを実施した。

2.4. アンケート調査結果の取りまとめ方

回答者の所属する企業規模については、従業員数 300 名未満（以下では中小企業等と呼ぶ）および従業員数 300 名以上（以下では大企業等と呼ぶ）で分類した。

3. 調査結果

3.1. 回答企業の概要

3.1.1. 業種

回答者の所属する企業等の業種については「他の製造業」（19.7%）が最も多く、「他のサービス業」（19.0%）、「情報通信業」（17.7%）、「小売業」（10.0%）が続く。

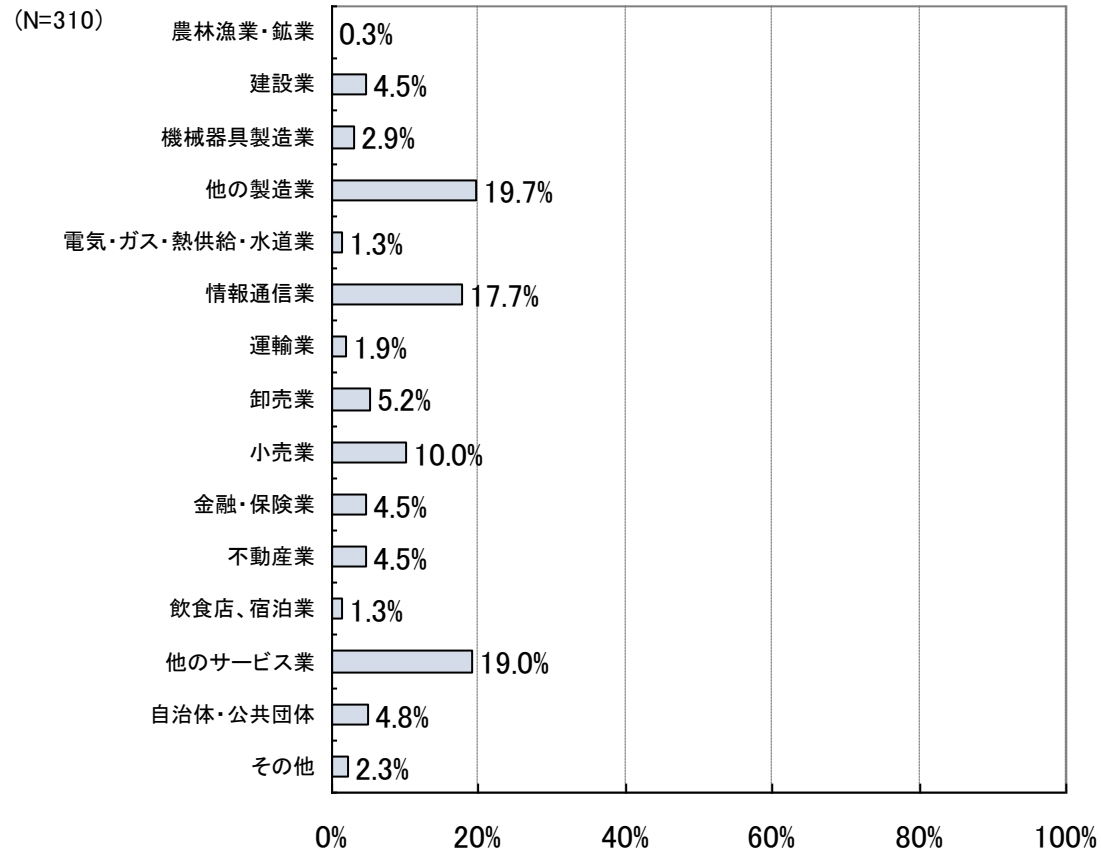

図 3.1-1　業種

注１）「他のサービス業」の回答の回収票については、属性情報を元に適切な業種への振り分けを可能な限り行った。

注２）標準産業分類に準じ、「情報通信業」に「情報サービス業」「放送業」「映像制作・新聞・出版業」を含む。また、「他のサービス業」には「医療・福祉業」「教育・学習支援業」を含む。

3.1.2. 総売上高（単体）

直近年度の総売上高（単体）は 5000 万円未満が 30%を占め、10 億円未満が約半数であった。

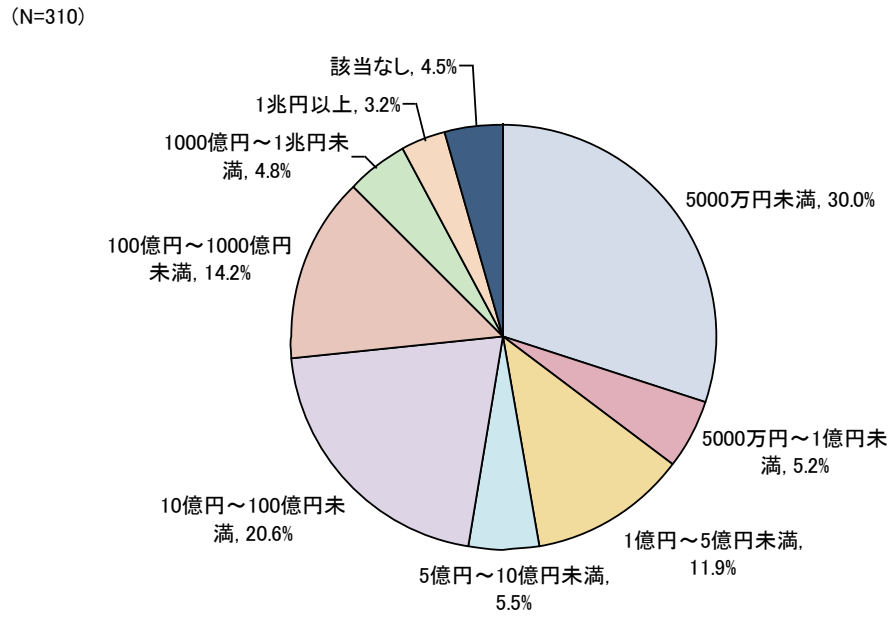

図 3.1-2　総売上高（単体）

注１）自治体・公共団体については予算額について回答を得た。

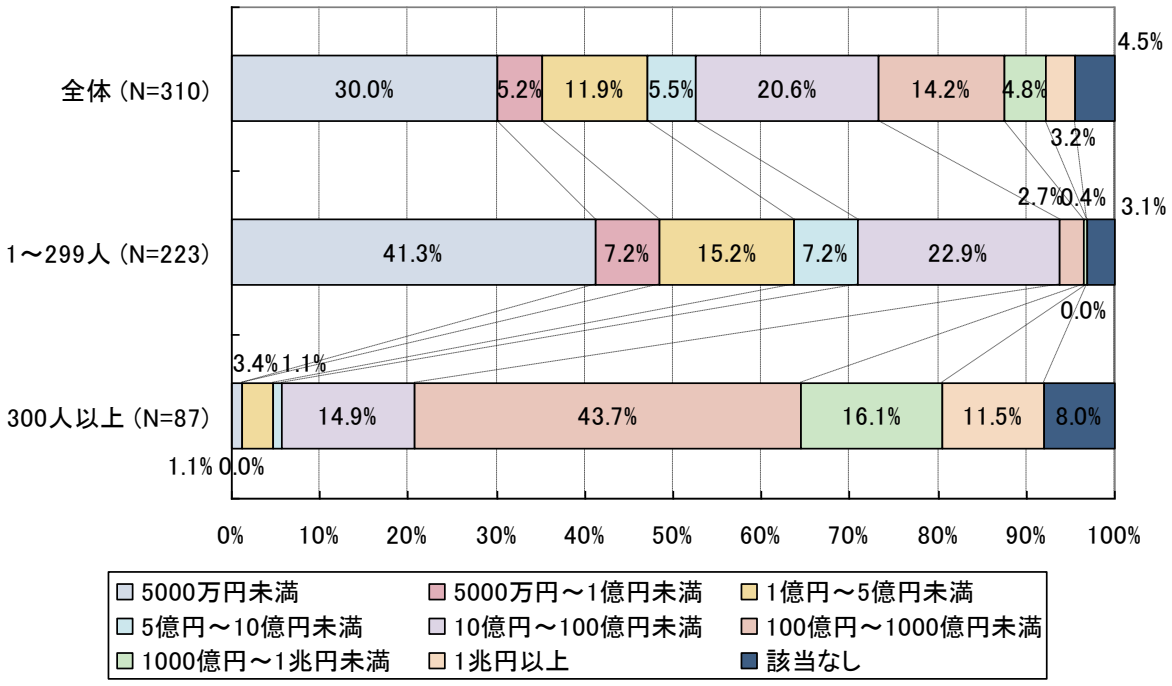

図 3.1-3　総売上高（単体、規模別）

注１）自治体・公共団体については予算額について回答を得た。

3.1.3. 事業所数

事業所数は「1 箇所のみ」（43.9%）との回答が最も多く、ついで「2 箇所～10 箇所」（33.5%）が多かった。

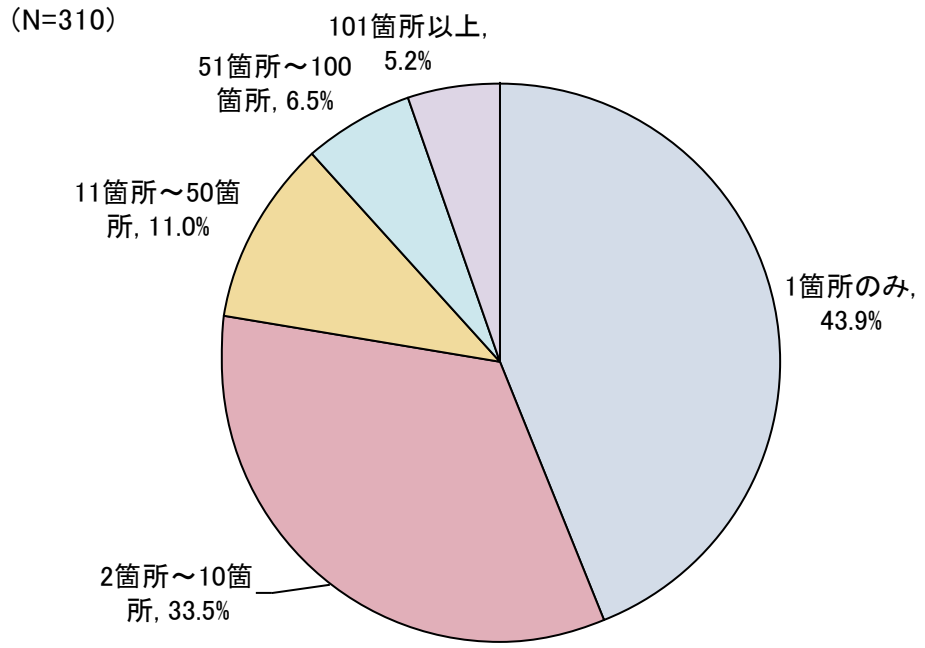

図 3.1-4　事業所数

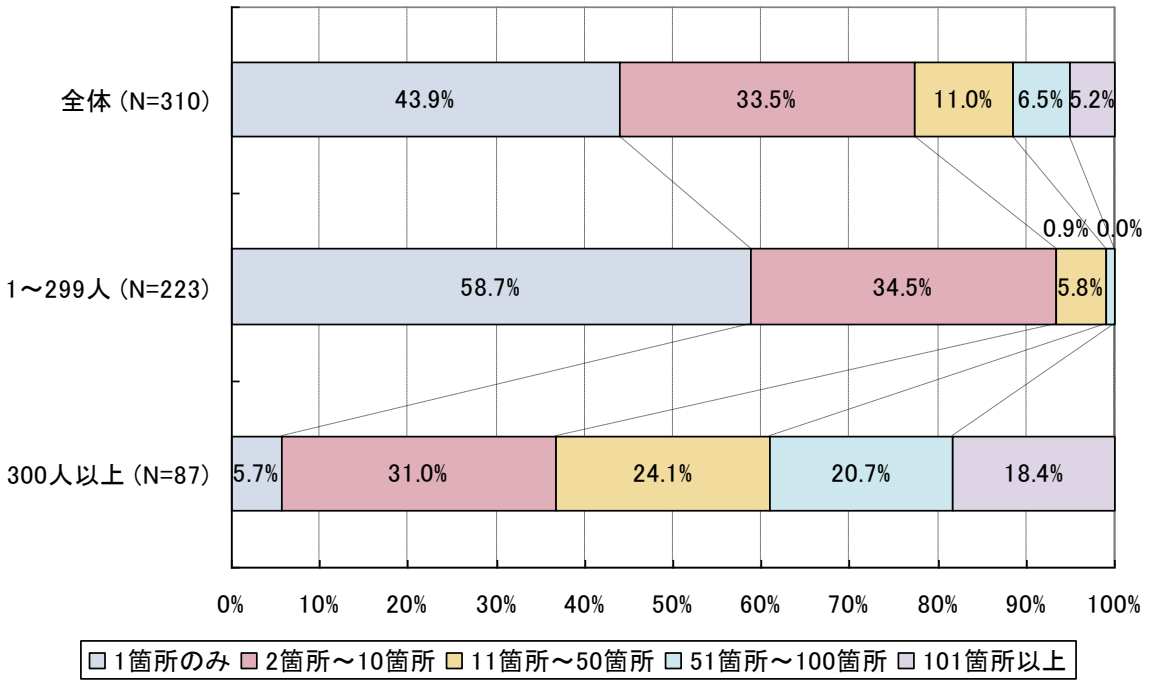

図 3.1-5　事業所数（規模別）

3.1.4. 従業員数・職員数

組織の従業員数については、1～9 人の組織が 32.9%を占め最も多く、300 人未満の組織は全体の約 7 割であった。

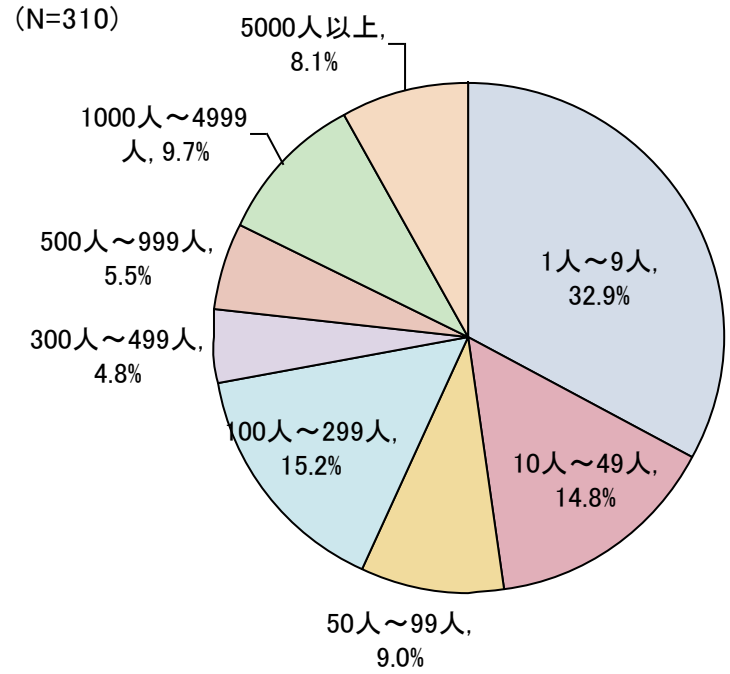

図 3.1-6　従業員数・職員数

注 1）従業員数・職員数についてはアンケートの設問への回答結果を用いず、調査対象者の属性データを基に集計した。

3.1.5. 回答者が担当する情報システム

回答者が企画・構築・運用・保守を担当している場合、どのようなシステムを対象としているかを尋ねた。全ての回答者（100.0%）が自組織のシステムの企画・構築・運用・保守を担当し、そのうちの 25.2%は顧客のシステムも担当している。

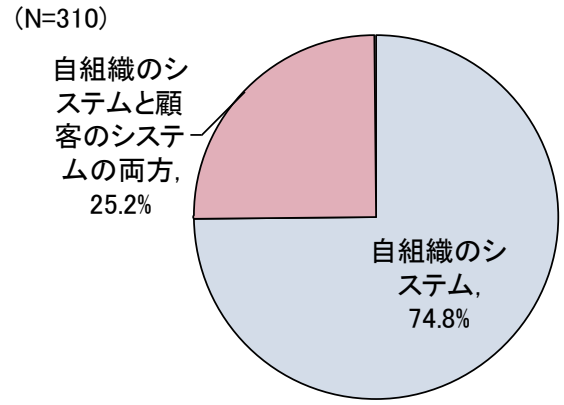

図 3.1-7　回答者が担当するシステム

さらに回答者が企画・構築・運用・保守に関与しているシステムの種類を尋ねた。どのシステムについても、関与する回答者が全体の 7 割を超えている。セキュリティ関連業務の担当者が幅広い種類のシステムに関与している様子が伺える。

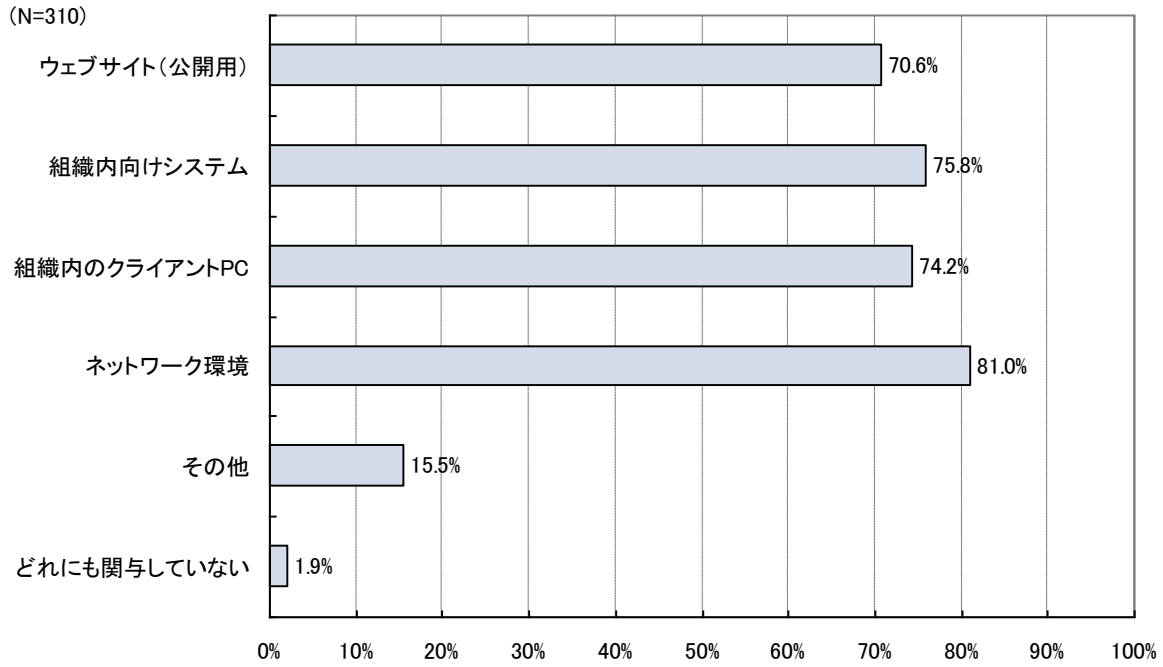

図 3.1-8　回答者が関与するシステムの種類（複数回答可）

3.1.6. 情報セキュリティ早期警戒パートナーシップの認知度

ソフトウェア等の脆弱性関連情報の届出や調整・公表を行う「情報セキュリティ早期警戒パートナーシップ」について知っているかを尋ねた。届出受付については 6 割程度と比較的知られていたものの、制度の枠組みや製品開発者調整については半数が知らなかった。

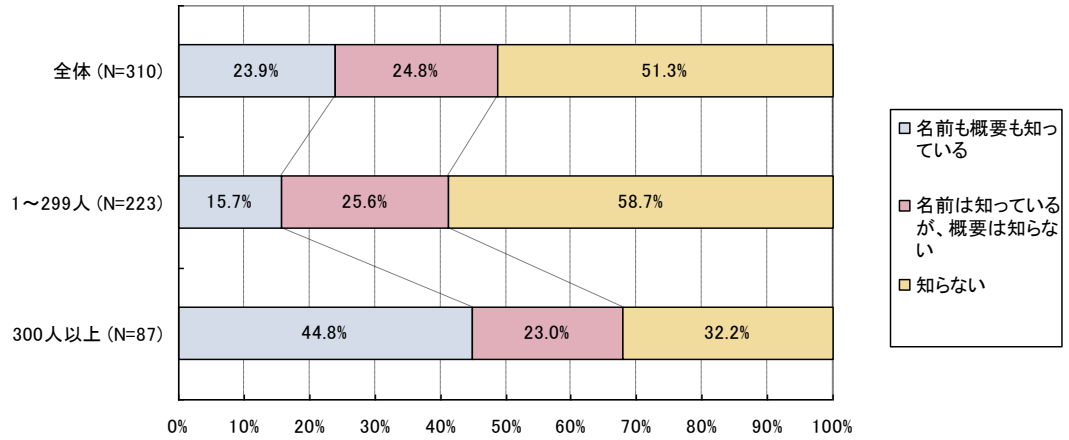

図 3.1-9 「情報セキュリティ早期警戒パートナーシップ」の認知度

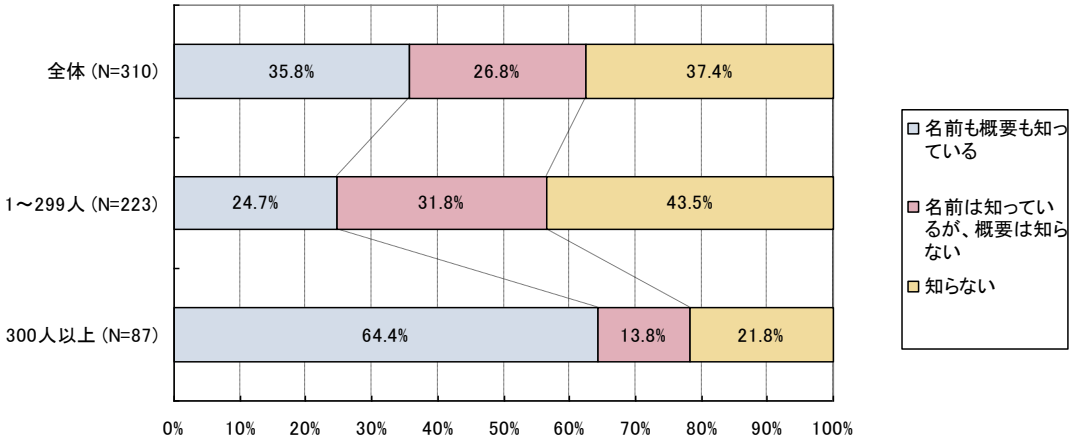

図 3.1-10 「脆弱性関連情報の届出受付（IPA)」の認知度

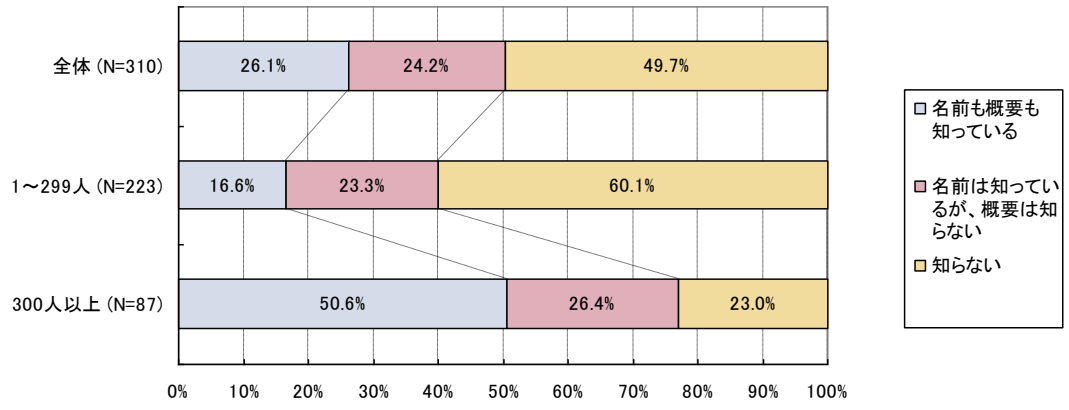

図 3.1-11 「製品開発者調整（JPCERT/CC)」の認知度

3.1.7. IPA 脆弱性関連事業の利用状況

IPA が実施する脆弱性関連事業の利用状況について尋ねた。いずれの事業も大企業等には 6 割ほど、中小企業等には 4 割ほどに知られている。利用経験があるとの回答は大企業等で 3 割から 4 割、中小の組織では 1 割程に留まった。

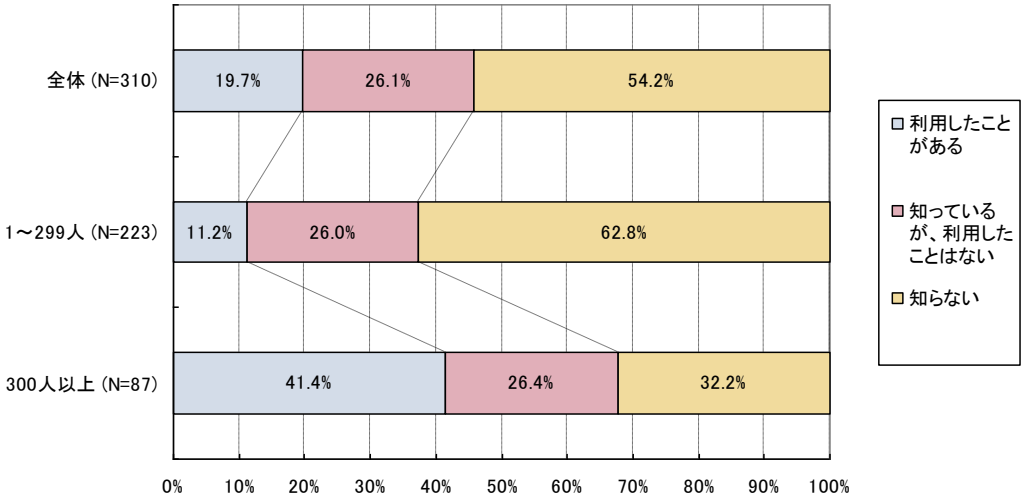

図 3.1-12 「JVN」の認知度

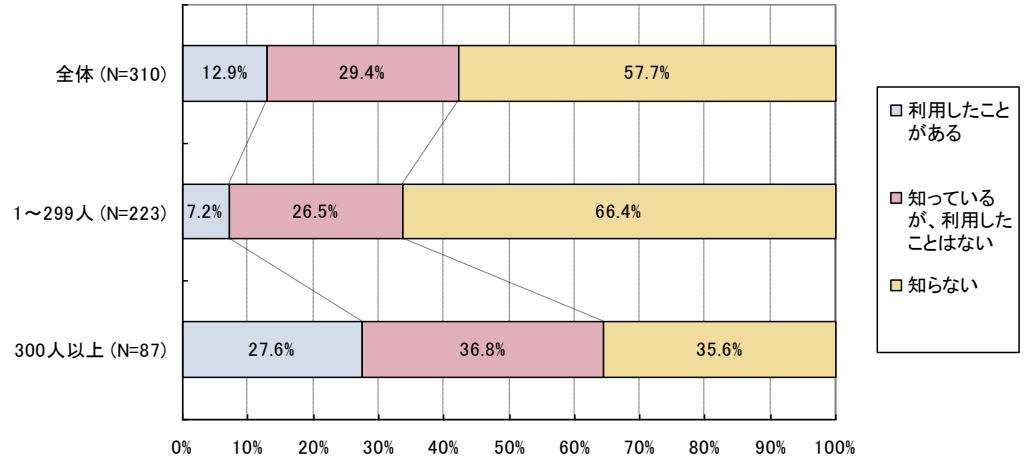

図 3.1-13 「MyJVN バージョンチェッカ」の認知度

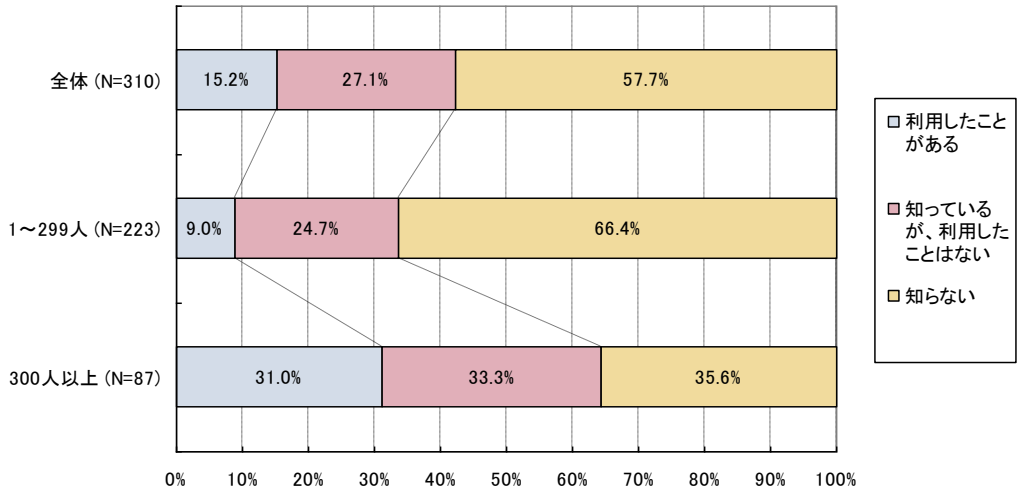

図 3.1-14 「MyJVN」の認知度

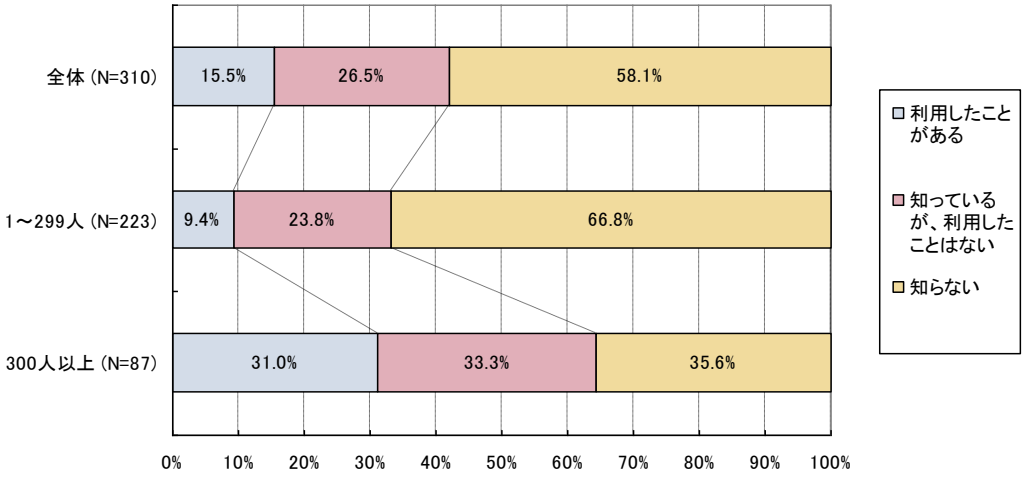

図 3.1-15 「安全なウェブサイトの作り方」の認知度

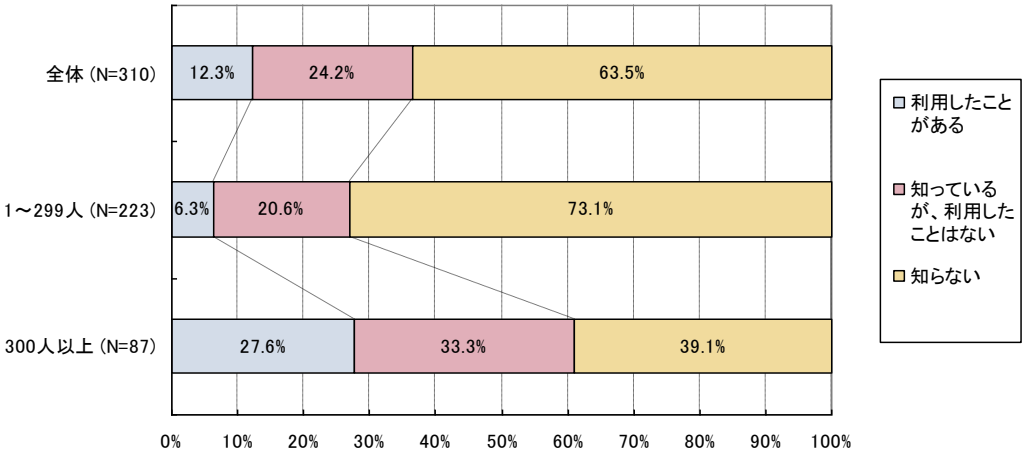

図 3.1-16 「10 大脅威 あぶりだされる組織の弱点！」の認知度

3.2. IT および情報セキュリティ対策全般の状況

3.2.1. IT 関連支出および IT 投資度

IT 関連の支出について、直近 1 年間にかけた費用の総額を尋ねたところ、「100 万円未満」と回答した企業が最も多く（46.1%）、次いで「100 万円～1000 万円未満」（19.4%）、「1000 万円～1 億円未満」（13.5%）の順であった。

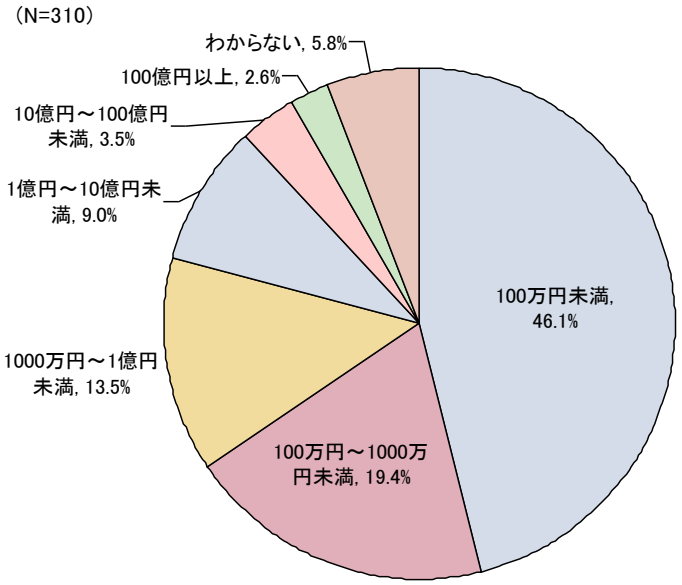

図 3.2-1　IT 関連支出（直近 1 年間）

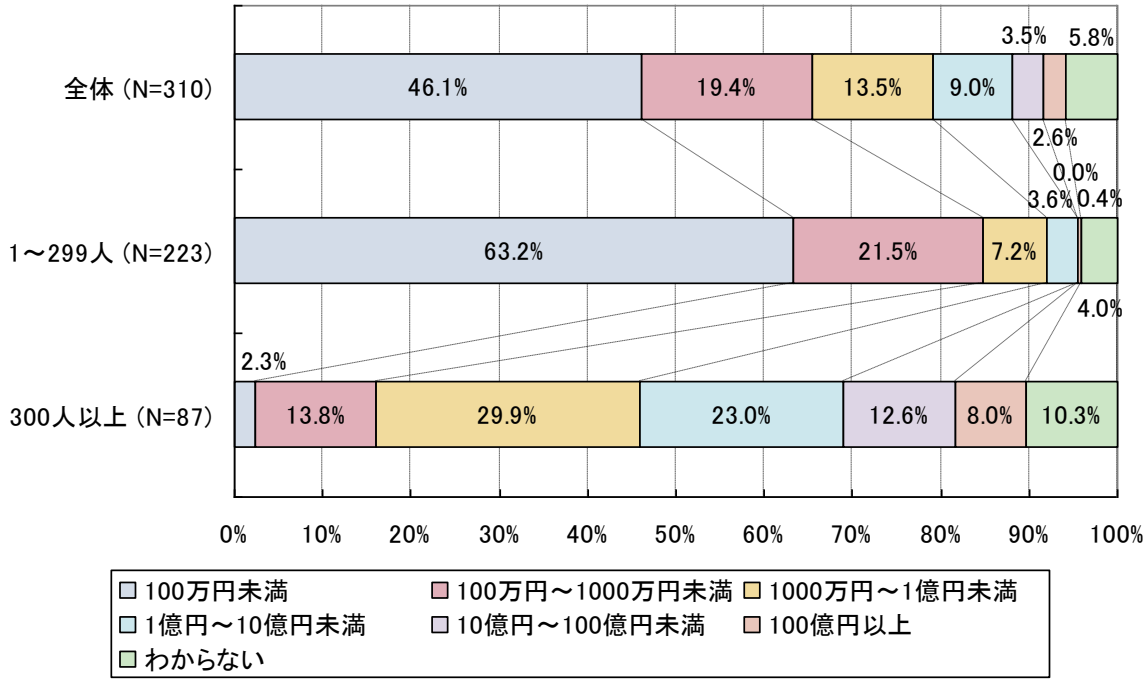

図 3.2-2　IT 関連支出（直近 1 年間、規模別）

この回答と先の「直近年度の総売上高」の回答を組み合わせ、直近年度の総売上高に対する IT 関連支出額の比を導出し、これを IT 投資率とした。

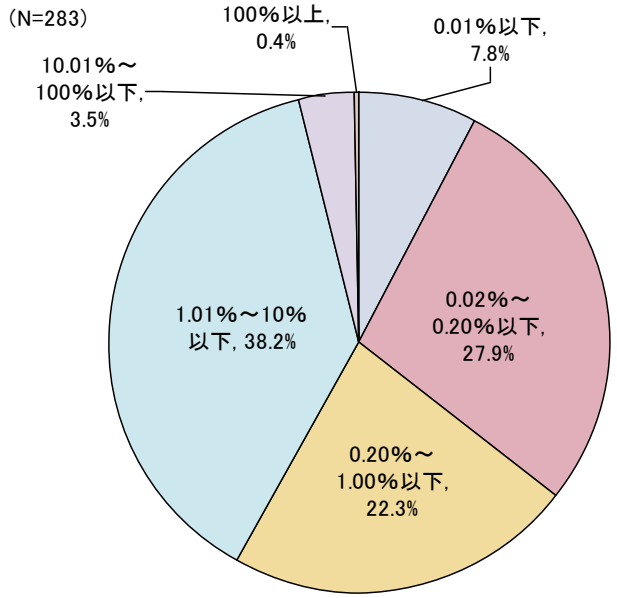

図 3.2-3　IT 投資率（直近 1 年間）

3.2.2. 情報セキュリティ支出率

直近 1 年間に情報セキュリティにかけた支出の総額が IT 関連支出の何%ほどかは、「1%未満」（25.8%）、「1%～5%」（25.8%）という回答が共に多く、これらが全体の半数を超えた。

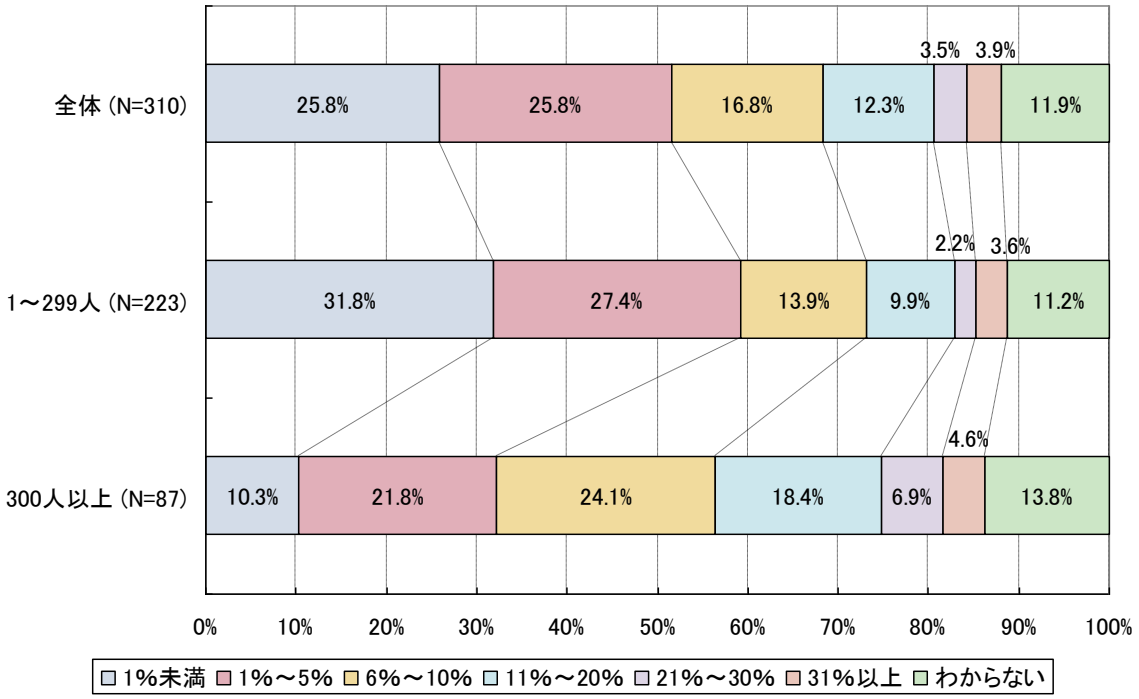

図 3.2-4　情報セキュリティ支出率（直近 1 年間、規模別）

3.2.3. 公開ウェブサイト数

組織がインターネットに公開しているウェブサイトの数は「1 サイトのみ」（52.9%）との回答が最も多く、次いで「2～5 サイト」（23.2%）、「公開していない」（11.6%）の順であった。

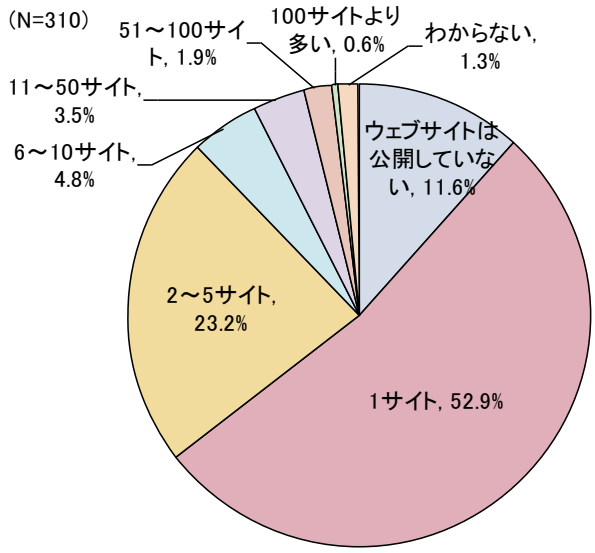

図 3.2-5　公開ウェブサイト数

3.2.4. 組織内向けサーバ数

利用している組織内向けサーバの数について尋ねたところ、およそ 8 割の組織でサーバを使っているとの回答を得た。約半数の組織では「1～10 台」の利用であった。

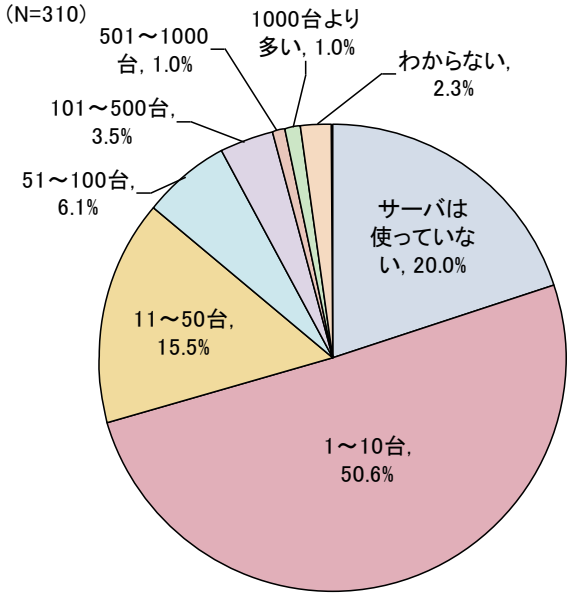

図 3.2-6　組織内向けサーバ数

注 1）ここでは、サーバ数は論理的な台数について回答を得た。仮想化されたサーバ（複数の仮想マシンを 1 台の物理マシン上で動かす手法等によるもの）については仮想マシンの台数を数えて加えている。

3.2.5. クライアント PC 数

組織で利用しているクライアント PC の数を尋ねたところ、およそ 9 割の組織ではクライアント PC は利用されている。

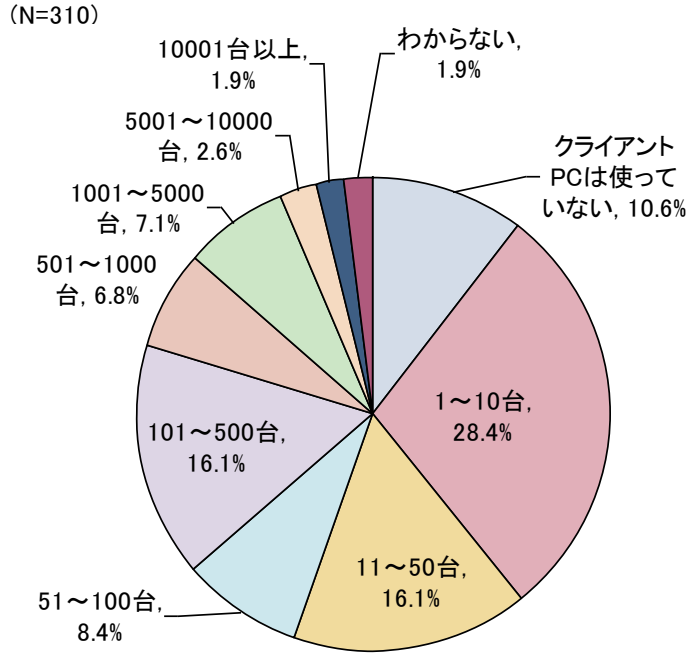

図 3.2-7　クライアント PC 数

3.2.6. 情報セキュリティ対策管理の体制

情報セキュリティ管理を行う部署や担当者が設置済みの組織は全体の 8 割を超える。特に大企業等においては、「情報セキュリティ管理を主担当とする部署がある」割合が 7 割以上を占め、「組織的には（情報セキュリティ対策管理を）行っていない」とする回答は皆無だった。

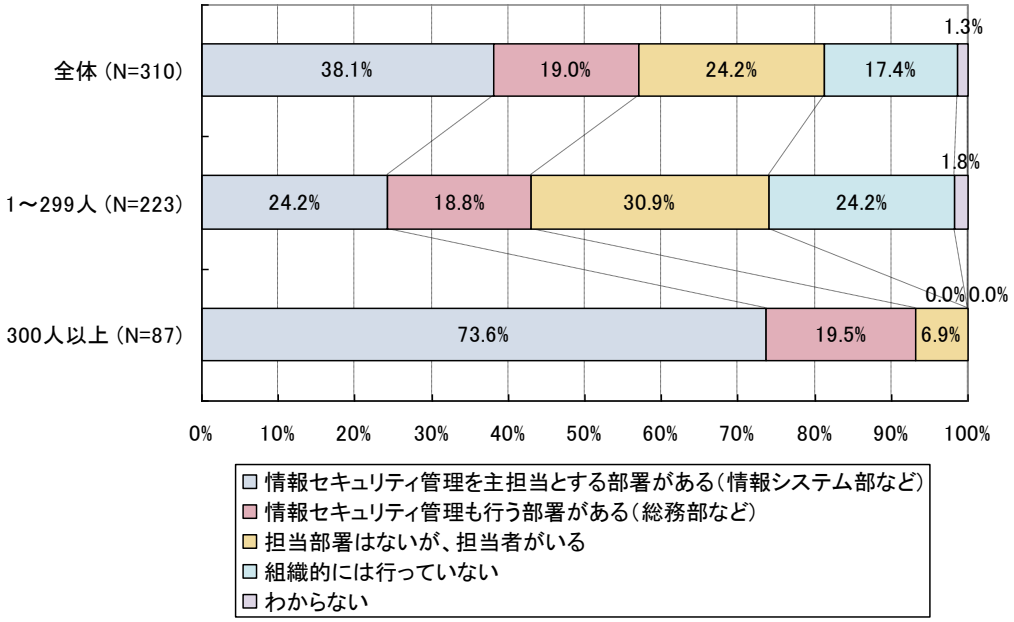

図 3.2-8　情報セキュリティ対策管理の体制（規模別）

3.2.7. 情報セキュリティ対策の外部委託

全体の 2 割ほどの組織において情報セキュリティ対策の外部委託が活用されている。特に、大企業等では 3 割を超える組織において外部委託が利用されている。

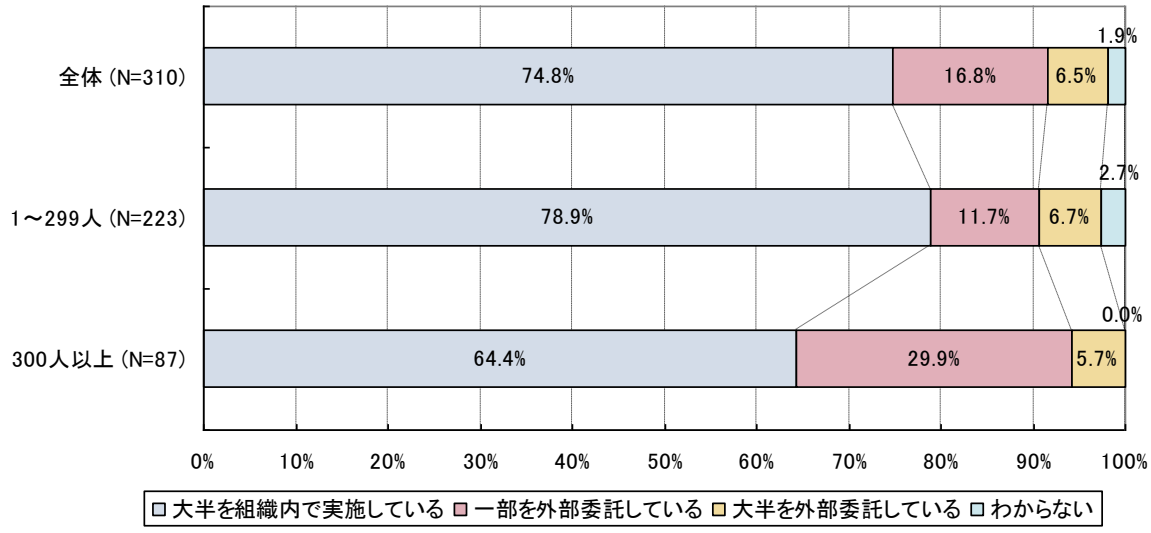

図 3.2-9　情報セキュリティ対策の外部委託の状況（規模別）

3.2.8. 情報セキュリティ教育の状況

情報セキュリティに関して組織で行っている教育について尋ねた。「関連情報の周知」が正社員等・準社員等のいずれでも 3 割以上の組織で行われている。「特に実施していない」とする組織もおよそ半数となっている。

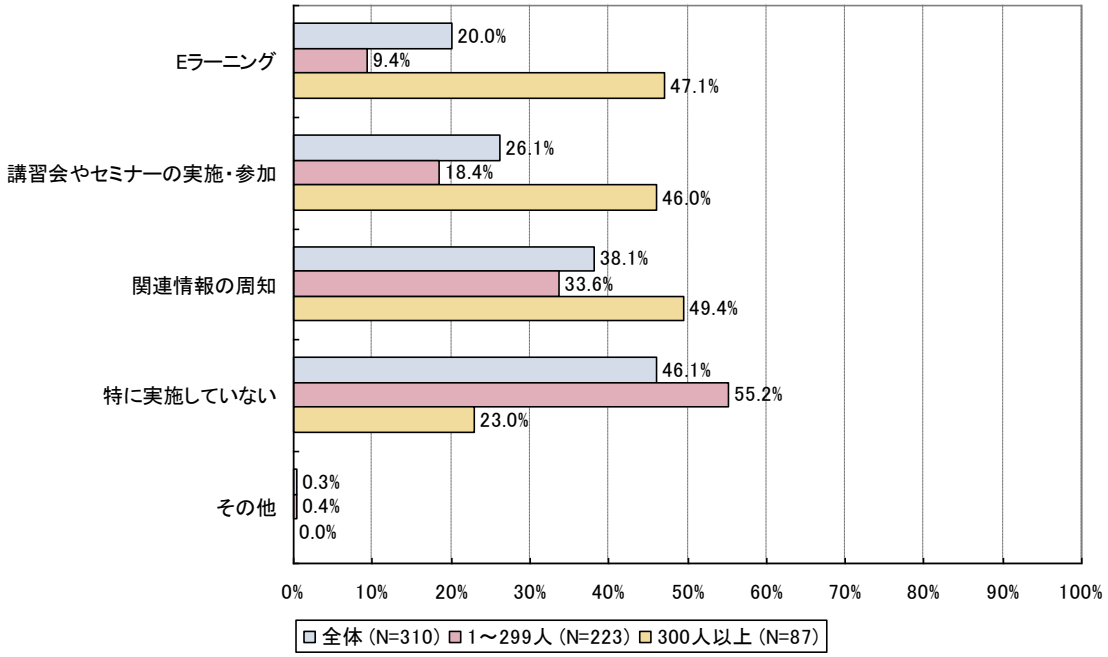

図 3.2-10　組織の情報セキュリティ教育（正社員・正職員）

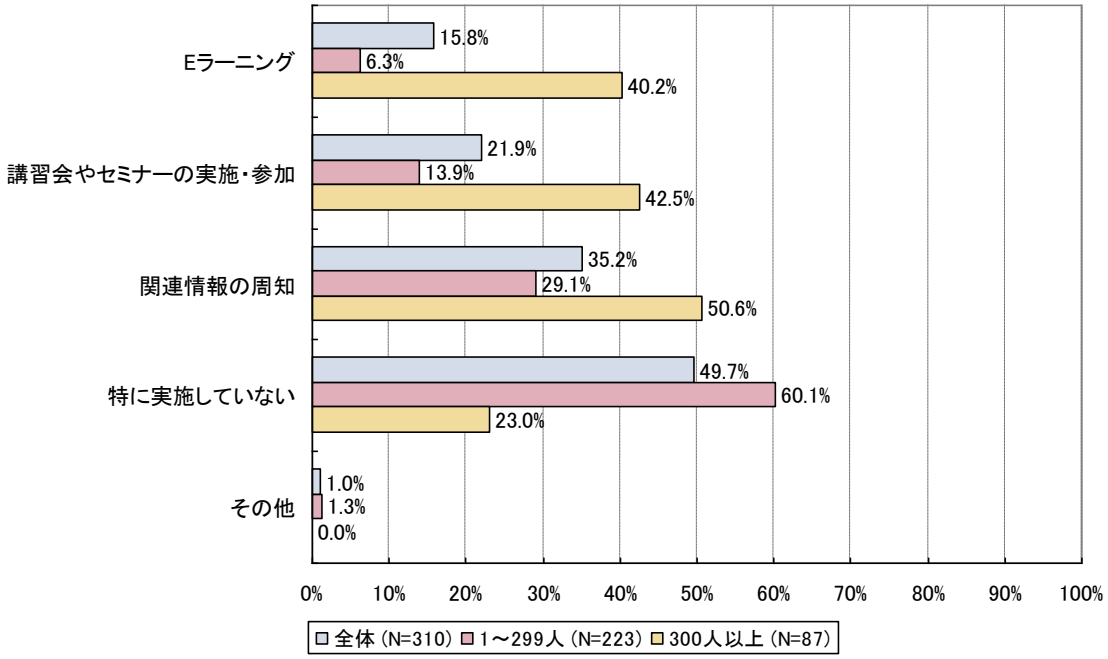

図 3.2-11　組織の情報セキュリティ教育（準社員・準職員・アルバイト）

3.3. 脆弱性とその対策に関する情報収集・分析の状況

3.3.1. 脆弱性情報の収集・確認担当者

組織において脆弱性に関する情報の収集・確認を主に行う者について尋ねた。およそ 8 割の組織で担当者を決めて実施されている。組織規模で見ると、大企業等では「情報収集を専任とする担当者」または「情報システム部門のスタッフ」がチェックするケースが 83.9%であるのに対して、中小の組織では 54.7%にとどまる。また、中小の組織では「特に決まっていない」とする回答が 24.7%と高い比率を示している。

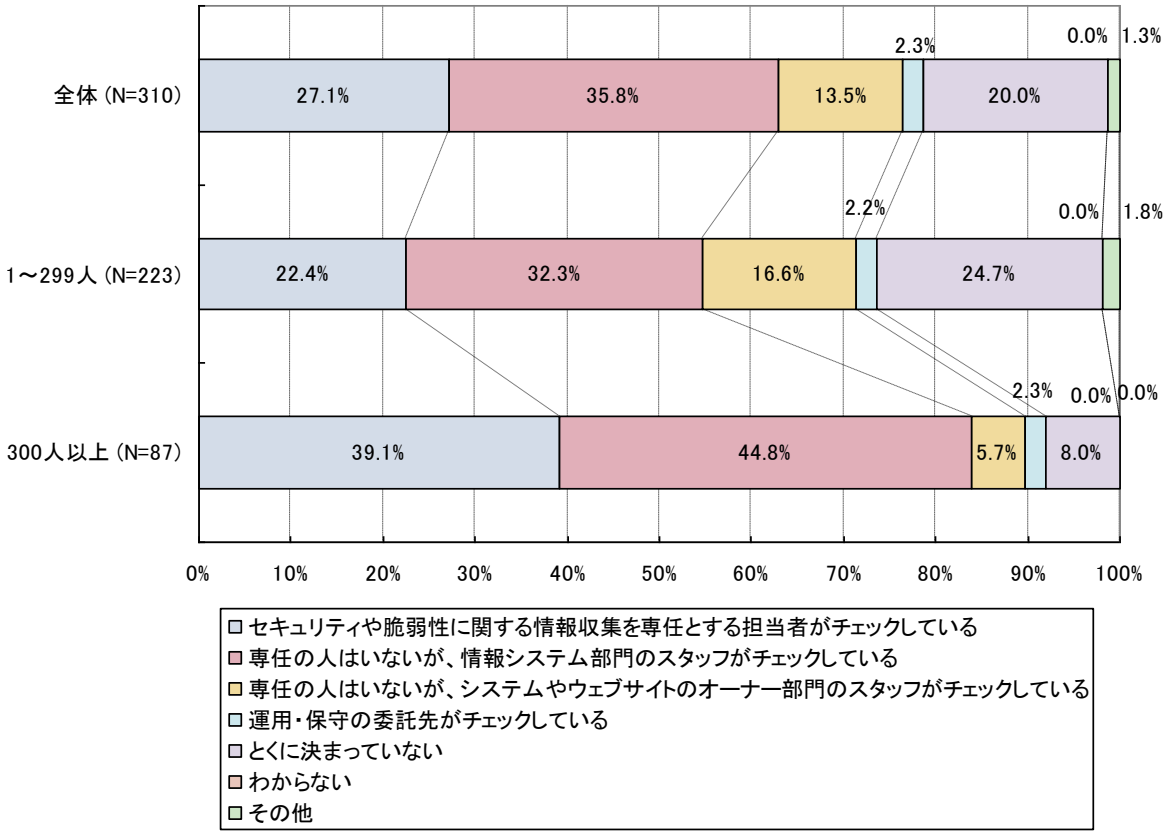

図 3.3-1　脆弱性情報の収集・確認担当者（規模別）

3.3.2. 脆弱性情報の入手元

脆弱性情報の入手元として活用する情報源を尋ねた。「ソフトウェア製品のメーカ」（50.6%）、「セキュリティ製品・サービスのベンダ」（50.0%）が多く挙がった。

特に「セキュリティ製品・サービスベンダ」、「SI 等、運用・保守事業者」、「国内のセキュリティ関連組織・ボランティア等」の項目については、中小企業等に比べ大企業等では回答する企業の割合が 20 ポイント程高く、企業規模による差異が見られた。

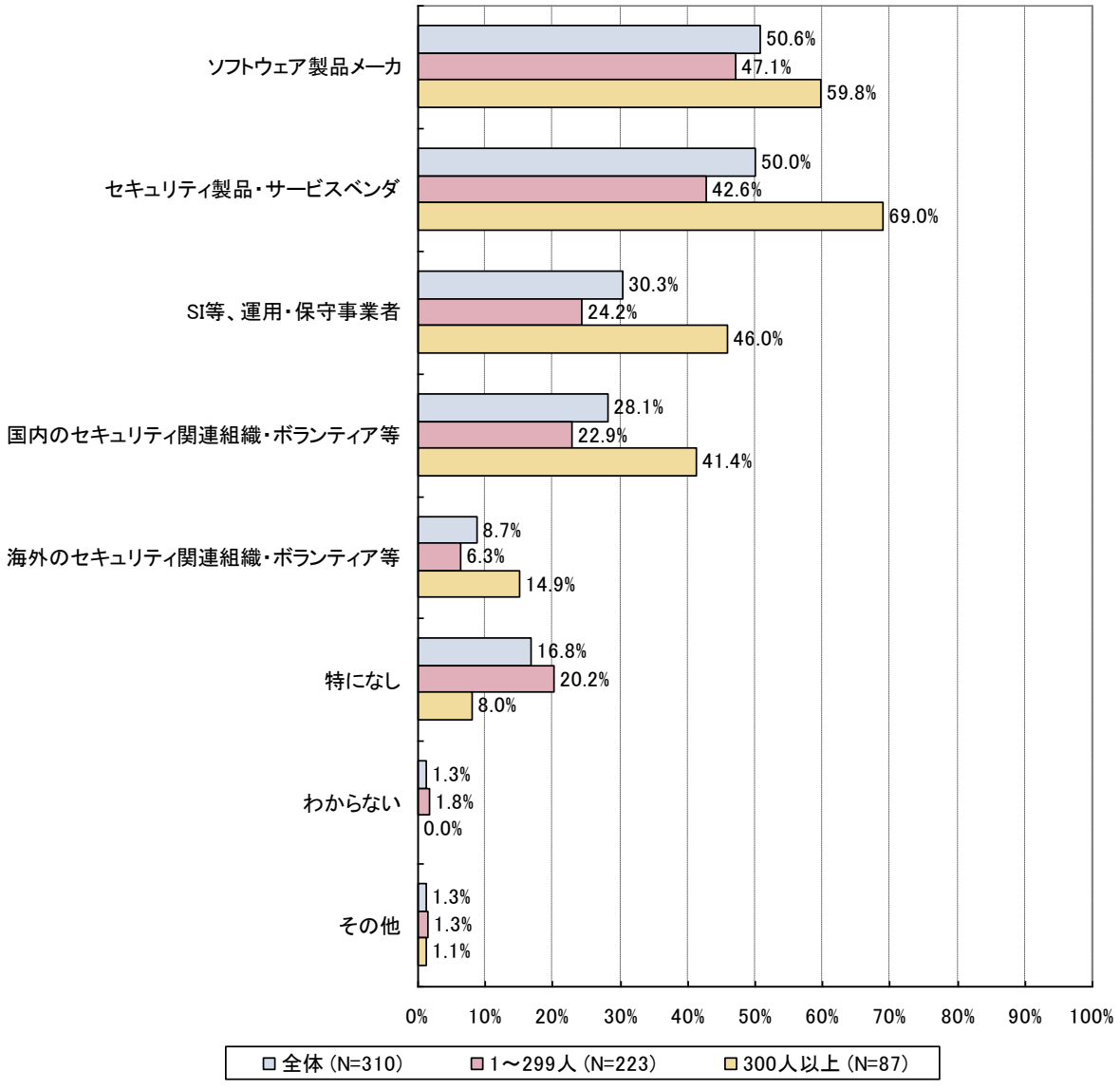

図 3.3-2　脆弱性情報の入手元（規模別）

3.4. ウェブサイトの脆弱性対策に関する状況

3.4.1. 開発・構築の状況

自組織でウェブサイトをどのように開発・構築しているかを尋ねたところ、「基本的に自組織で構築している」組織は 6 割程であり、外部事業者に委託している組織は 3 割程であった。また、大企業等は中小企業等に比べ開発・構築を外部委託する割合が高かった。

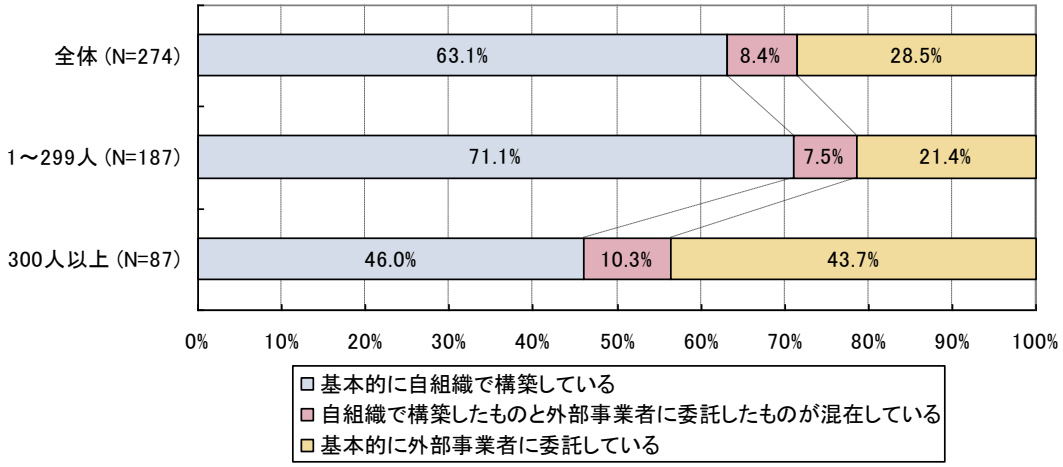

図 3.4-1　ウェブサイト開発・構築の状況（規模別）

3.4.2. 運用・保守の状況

ウェブサイトを「基本的に自組織で運用・保守している」組織が 7 割であり、外部事業者に運用・保守を委託している企業はおよそ 3 割であった。また、大企業等は中小企業等に比べ運用・保守を外部委託する割合が高かった。

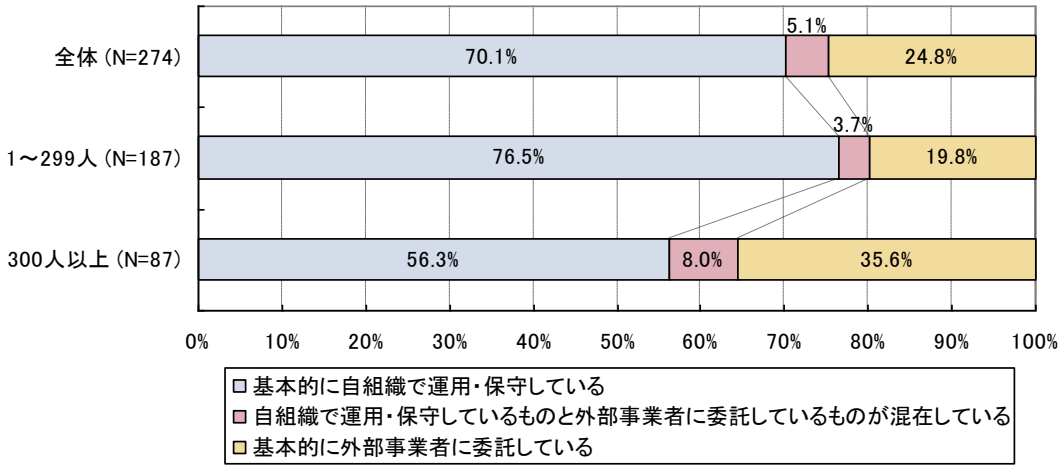

図 3.4-2　ウェブサイト運用・保守の状況（規模別）

外部事業者に委託していると回答した組織に、主にどんな作業を外部に委託しているかを尋ねたところ、「システム保守」（78.0%）、「コンテンツ更新・制作」（61.0%）という回答が過半数より得られた。

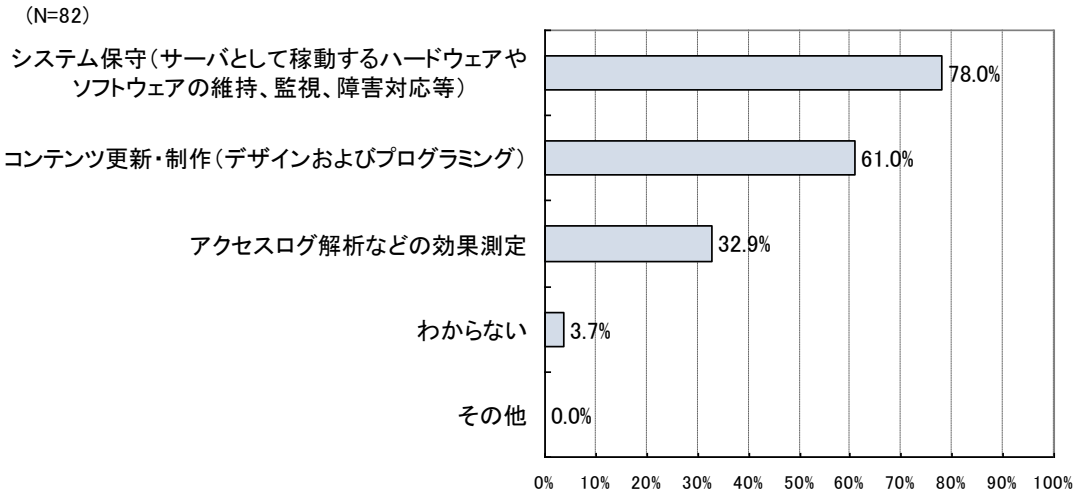

図 3.4-3　ウェブサイト保守等で外部委託する内容

3.4.3. 構築時の脆弱性対策

ウェブサイト構築時に脆弱性対策をどのように行っているかを尋ねた。構築の時点で脆弱性対策を行っている組織は大企業等で 65.5%あるのに対し、中小企業等では 35.3%にとどまる。

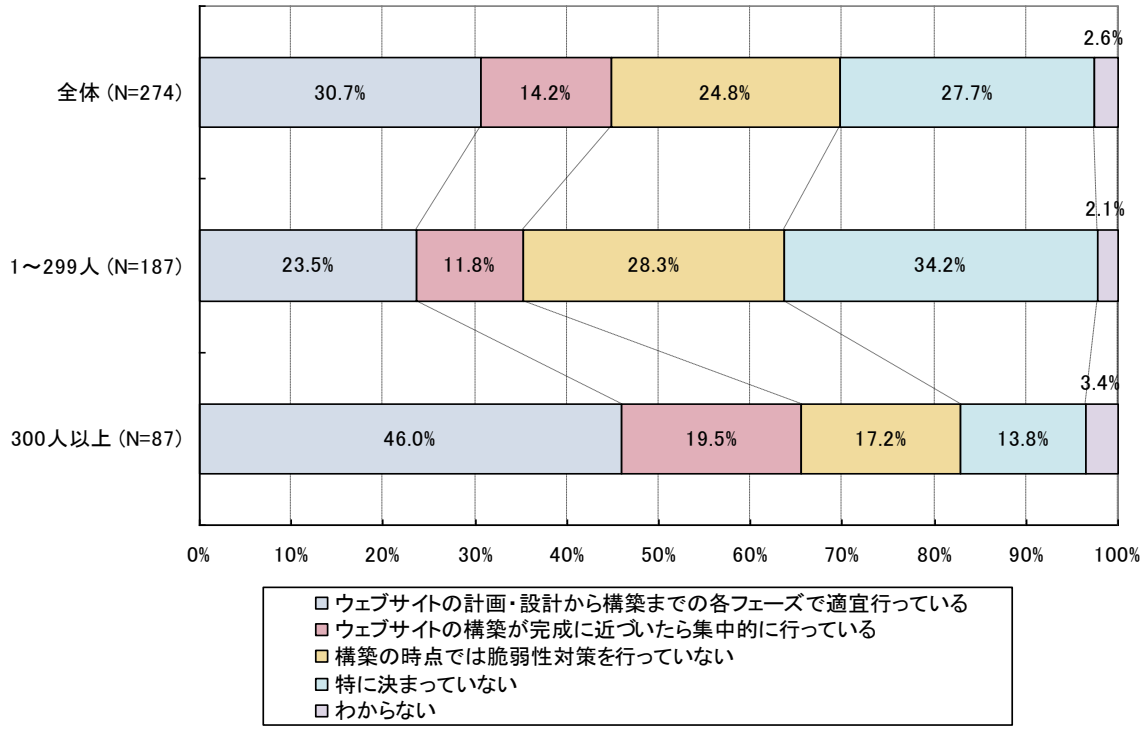

図 3.4-4　ウェブサイト構築時の脆弱性対策（規模別）

3.4.4. 脆弱性検査や脆弱性診断サービスの利用状況

運用中のウェブサイトへの脆弱性検査等や脆弱性診断サービスの利用について尋ねた。自組織内の検査と外部サービス利用を合わせると全体では 5 割を超える組織で行われており、特に大企業等での実施率は 8 割近い。

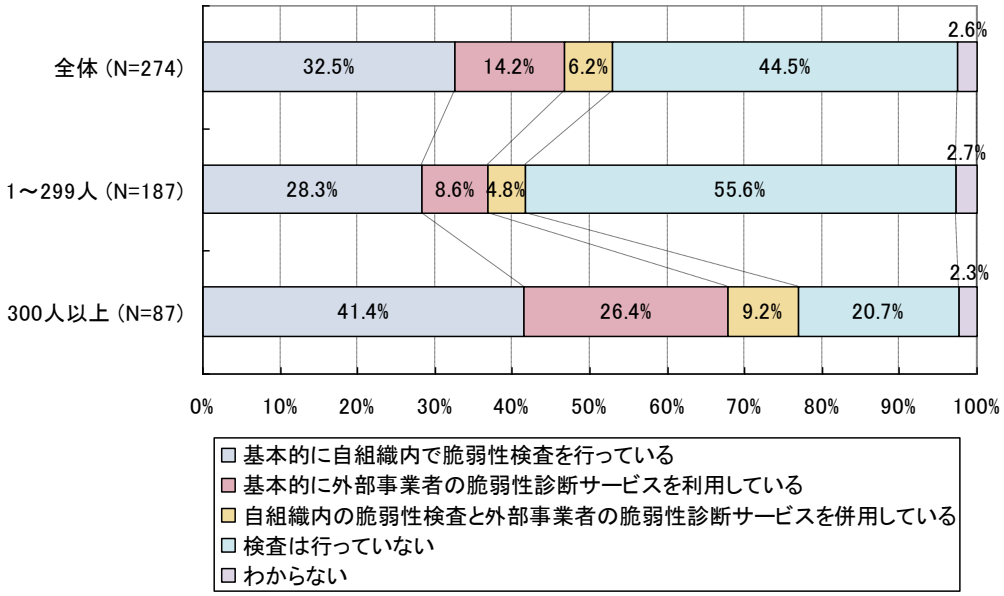

図 3.4-5　ウェブサイト脆弱性検査・診断サービスの利用状況（規模別）

さらにウェブサイトの脆弱性検査や脆弱性診断サービスを行っていると答えた組織を対象に利用頻度についても尋ねた。「ウェブサイトの構築時や改変時に併せて行っている」との回答が最も多く 56.6%であった。「定期的に行っている」とした組織は 18.6%に留まった。

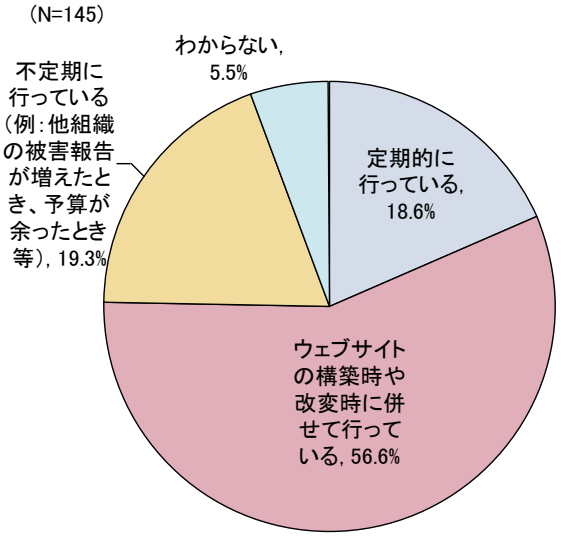

図 3.4-6　ウェブサイト脆弱性検査・脆弱性診断サービスの利用頻度

3.4.5. 脆弱性に気付くきっかけ

運用中のウェブサイトにおいて、脆弱性対策が必要な箇所について気付くきっかけを尋ねた。大企業等では、「セキュリティ関連組織等から連絡を受けた」、「脆弱性検査や脆弱性診断サービスを通じて気付いた」、「脆弱性による情報を入手して、自組織で確認し気付いた」、「組織外の関係者や取引先から連絡を受けた」の各選択肢は35～40%程度の回答者が選択しており、中小企業等に比べ高い比率であった。特に、「セキュリティ関連組織等から連絡を受けた」ケースが最も多く、情報セキュリティ早期警戒パートナーシップの取り組みが効果を挙げていることがわかる。

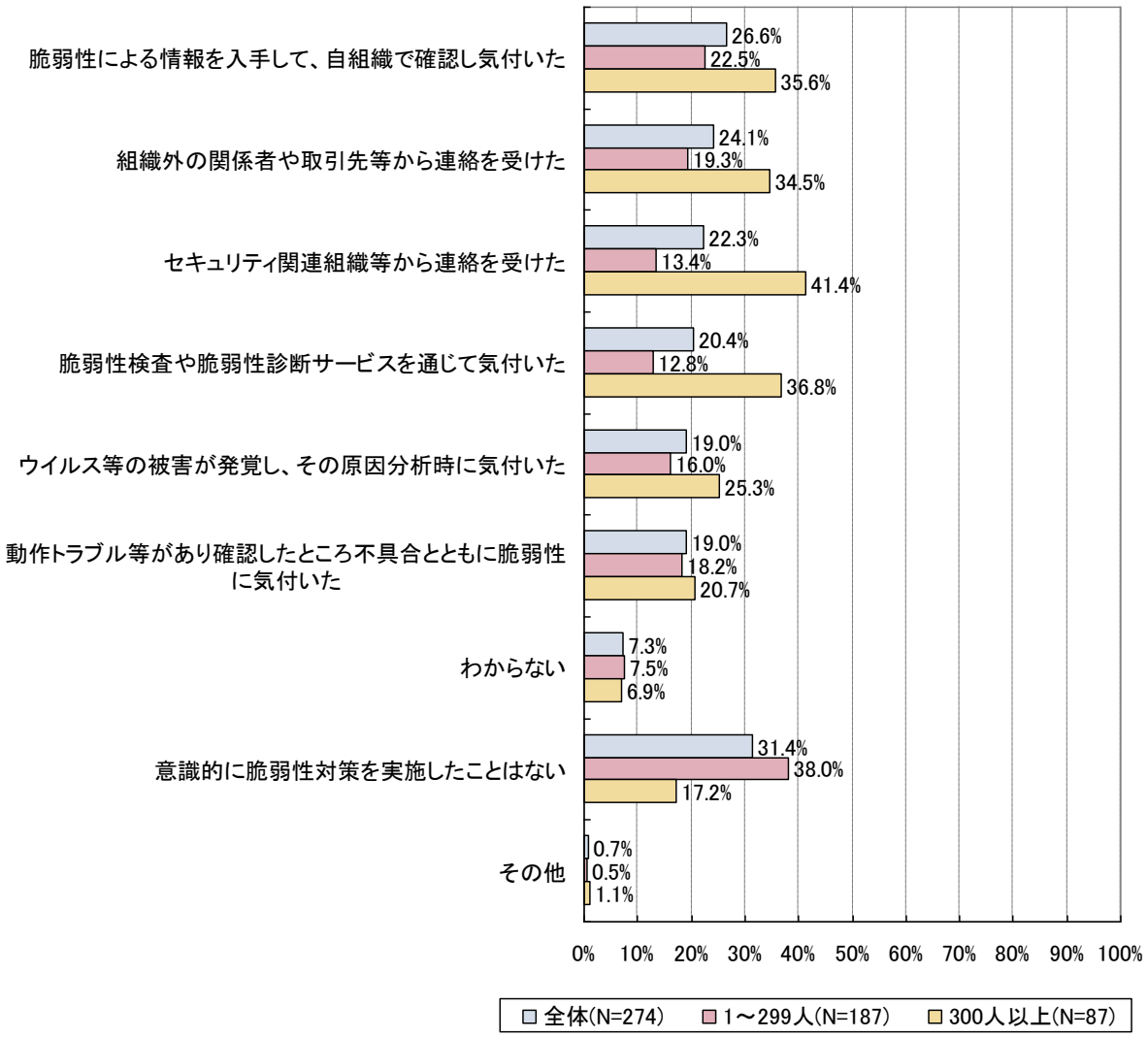

図 3.4-7 ウェブサイト脆弱性に気付くきっかけ（規模別）

3.4.6. 脆弱性対策の判断時に参考とする情報

ウェブサイトの脆弱性について対策を適用すべきか否か等を判断する際に参考とする情報について尋ねた。「セキュリティ関連製品・サービスベンダが示す脅威レベルの評価」を参考とする組織は全体の 4 割ほどであった。「セキュリティ関連組織等が提供する情報」を参考とする組織は全体の 2 割ほどであったが、大企業等だけで見ると 3 割を超える。つまり、IPA や JPCERT/CC からの情報は、大企業等においてより活用されていると言える。

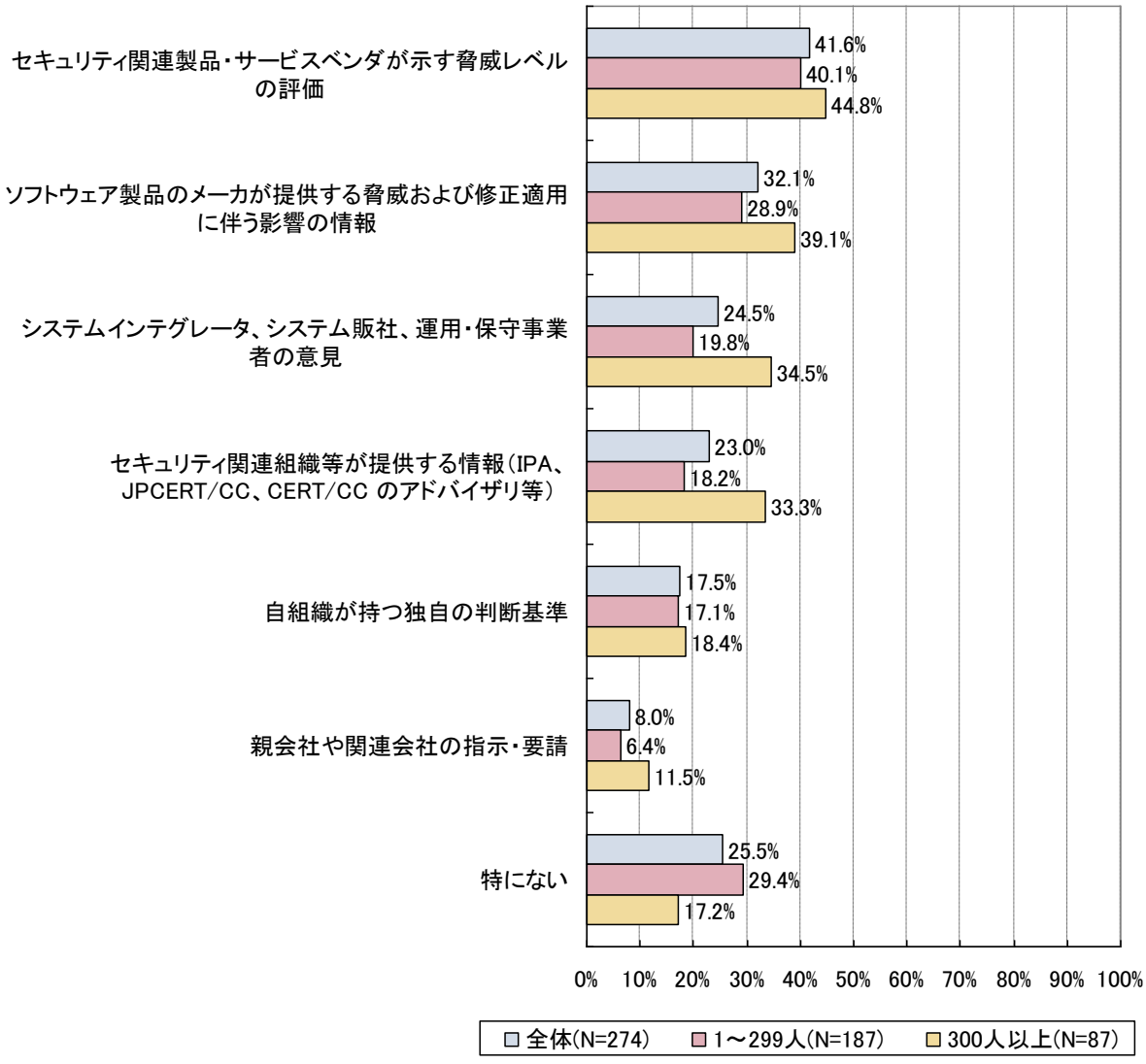

図 3.4-8　ウェブサイト脆弱性対策の判断時に参考とする情報（規模別）

3.4.7. 脆弱性対策の適用を判断する人

ウェブサイトの脆弱性対策を適用すべきか否か等を判断する人について尋ねた。全体のおよそ 8 割の組織においては判断する人は定められている。「情報セキュリティ管理の担当部署の責任者」が 32.5%で最も多く、「CIO/CISO 等、組織全体の責任者」（17.5%）、「情報セキュリティ管理の実施担当者」（16.1%）が続く。

大企業等では、脆弱性対策の適用を判断する者として「情報セキュリティ管理の担当部署の責任者」を挙げる回答が 52.9%と最も多く、担当部署の職務として定められている場合が多い様子が伺える。一方、中小企業等では「特に決まっていない」（27.3%）とする割合が最も高く、対策に関する組織的対応が未整備なケースが多いと考えられる。

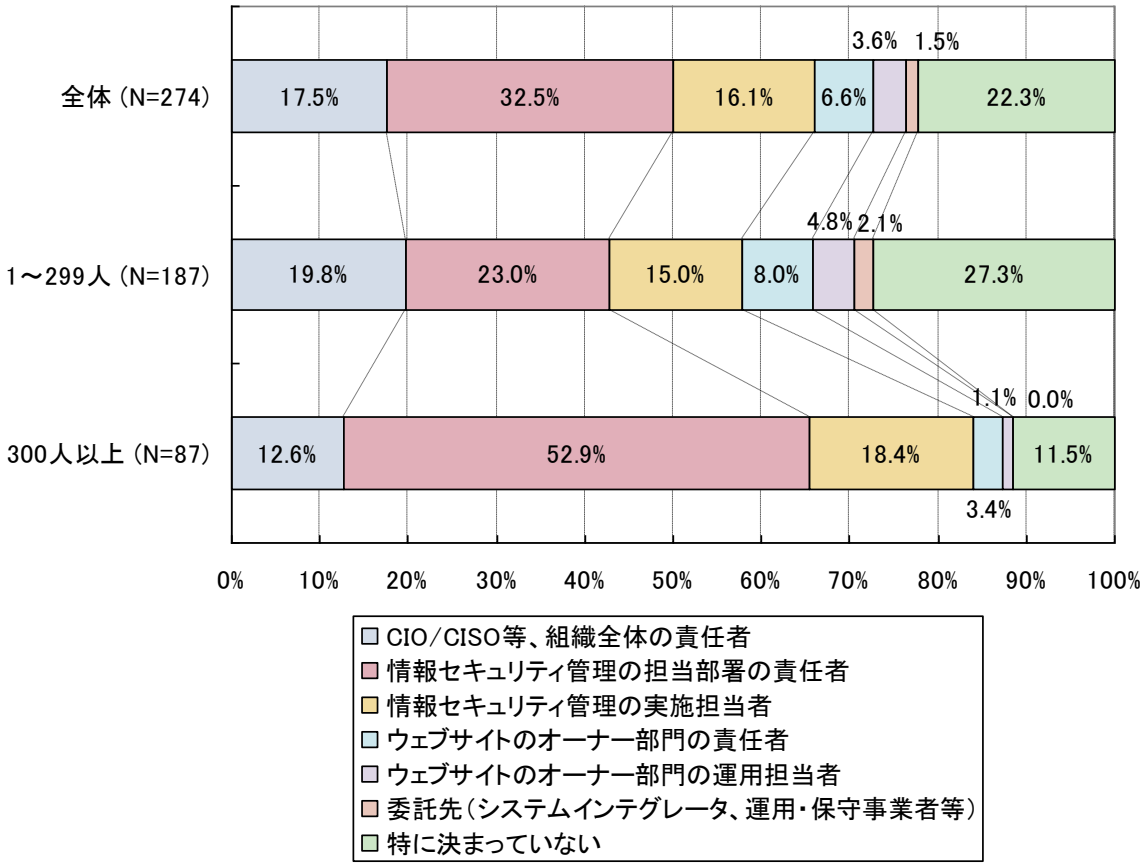

図 3.4-9　ウェブサイト脆弱性対策の適用を判断する人（規模別）

3.4.8. 脆弱性に関する対処手順の整備状況

ウェブサイトに関する脆弱性情報の収集、脆弱な箇所の特定と報告（外部からの発見報告を受領した場合を含む）、対処方針の決定、対策実施といった一連の手順を文書化しているかを尋ねた。大企業等においては対処手順を約 4 割の組織が「組織内ルールとして文書化」している一方で、中小企業等においては約 1 割しか文書化しておらず、逆に 7 割以上の組織が「特に定まった手順がない」としている。

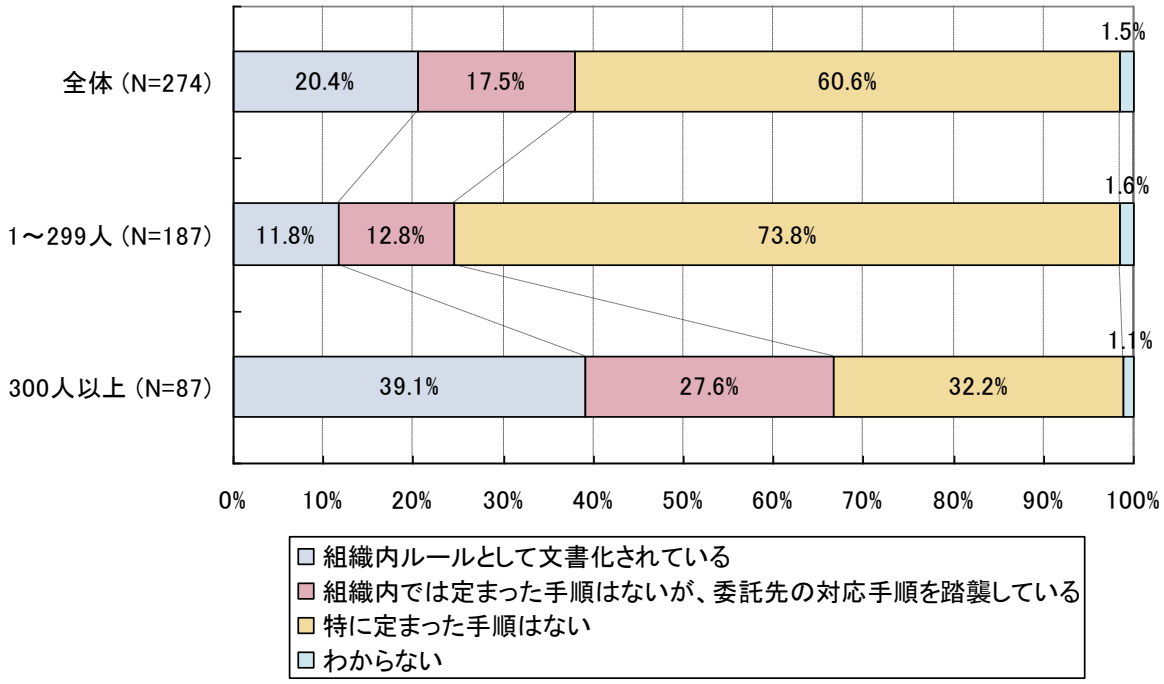

図 3.4-10　ウェブサイト脆弱性に関する対処手順の整備状況（規模別）

3.4.9. 脆弱性が関係する不正アクセス等の被害経験

ウェブサイトの脆弱性対策における遅れやミスが間接的な原因となって、不正アクセス等の被害に遭った経験の有無について尋ねた。被害経験は中小企業等では 14.9%にとどまるのに対し、大企業等では 47.1%に達し、その約半分は「複数部門の業務に影響が生じる被害が発生した」経験を有する。

この結果は、著名企業等のほうがウェブサイトを狙われやすいこと、またセキュリティ対策が進むと被害を把握しやすくなることが影響したものと考えられる。

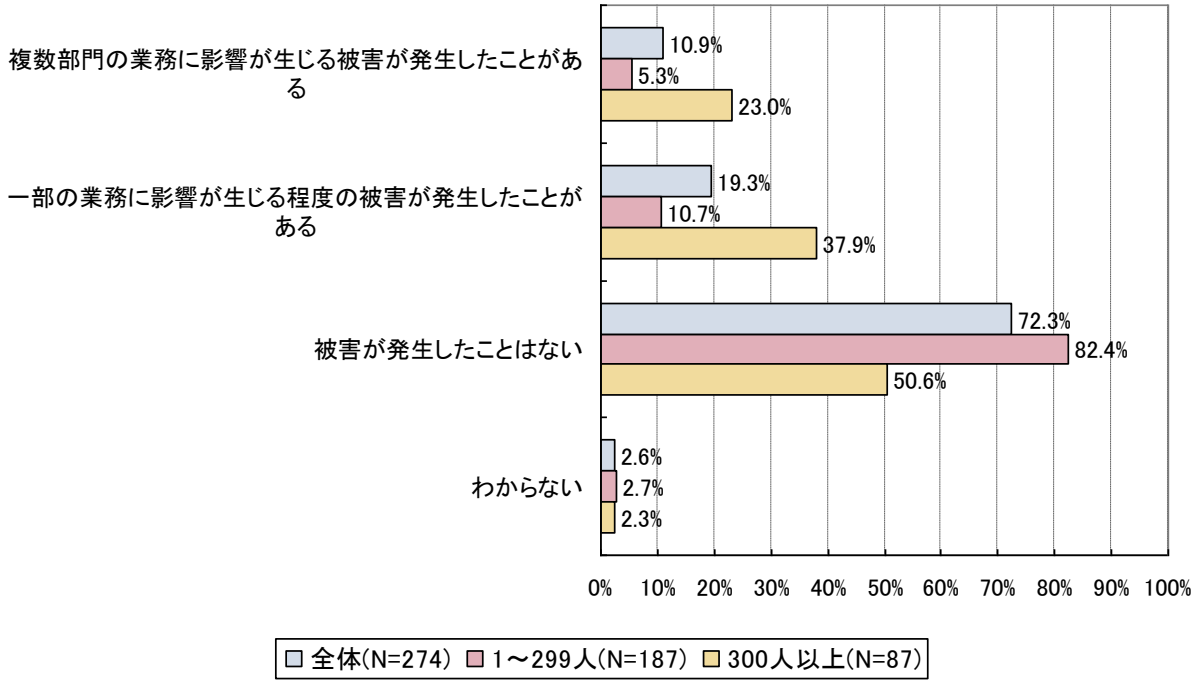

図 3.4-11　ウェブサイト脆弱性が関係する不正アクセス等の被害経験（規模別）

3.4.10. 修正適用の作業担当者

運用中のウェブサイトにおける脆弱性の修正や回避策の適用等の作業の主担当者について尋ねた。「情報セキュリティ管理の実施担当者」（全体の 55.5%）が最も多く、次いで「ウェブサイトのオーナー部門」（20.8%）という回答であった。組織規模による差異はわずかであった。

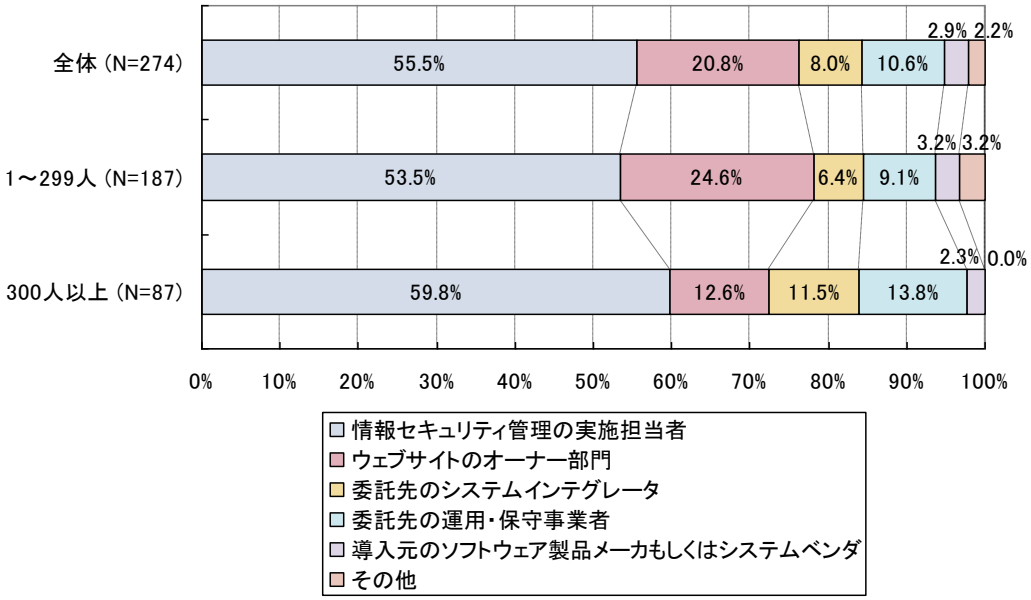

図 3.4-12　ウェブサイト修正適用の作業担当者（規模別）

さらに上の設問で外部組織と回答した者を対象に、運用中のウェブサイトの脆弱性対策に必要な契約と費用について確認した。脆弱性対策について契約には明記されていないものの事実上委託費用に全て含まれているとした回答が最も多く（33.8%）、委託先との契約に明記されているとした回答は 24.6%にとどまる。

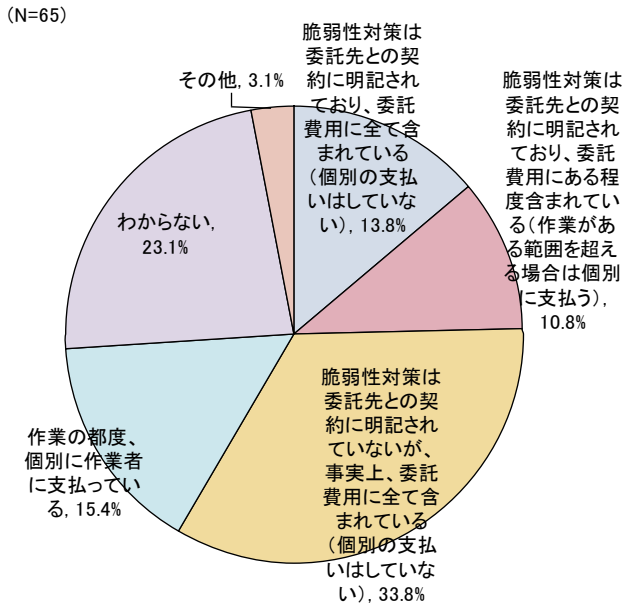

図 3.4-13　運用中のウェブサイトの脆弱性対策に関する契約と費用負担

3.4.11. 具体的な脆弱性への対策状況

より具体的に対策実態を把握するために、ウェブサイトにおいて見られる典型的な脆弱性について組織全体として対策を取っているかを尋ねた。いずれの項目についても 3 割程度において「対策済み」との回答が得られた。

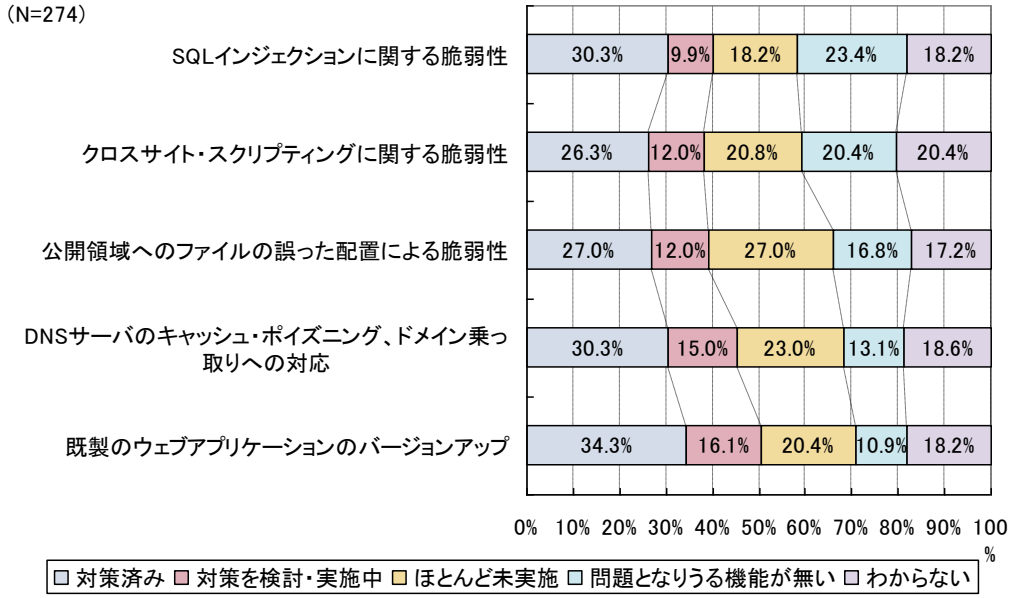

図 3.4-14　ウェブサイト脆弱性への対策状況

3.4.12. WAF の利用状況

ウェブサイトの脆弱性対策として WAF（ウェブ・アプリケーション・ファイアウォール）を利用している組織は中小企業等の 24.1%、大企業等の 48.2%に達している。WAF を利用している組織の 3 分の 1 は「ウェブアプリケーションの修正を行わない」との回答であった。

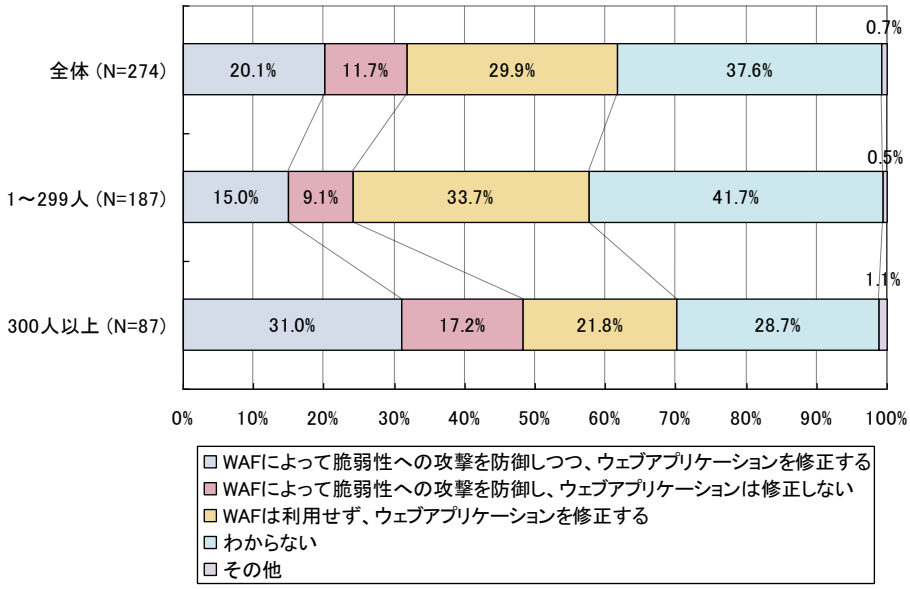

図 3.4-15　WAF の利用状況（規模別）

3.4.13. 脆弱性を修正するタイミング

ウェブサイトの脆弱性を修正するタイミングは、大企業等では「脆弱性について情報が得られるたびに実施」（26.4%）とする組織が最も多く、次に「緊急性の高いものだけを即時実施し、それ以外は状況に応じて適宜実施」（25.3%）が続く。中小企業等では「状況に応じて適宜実施」（25.7%）の割合が最も高い。

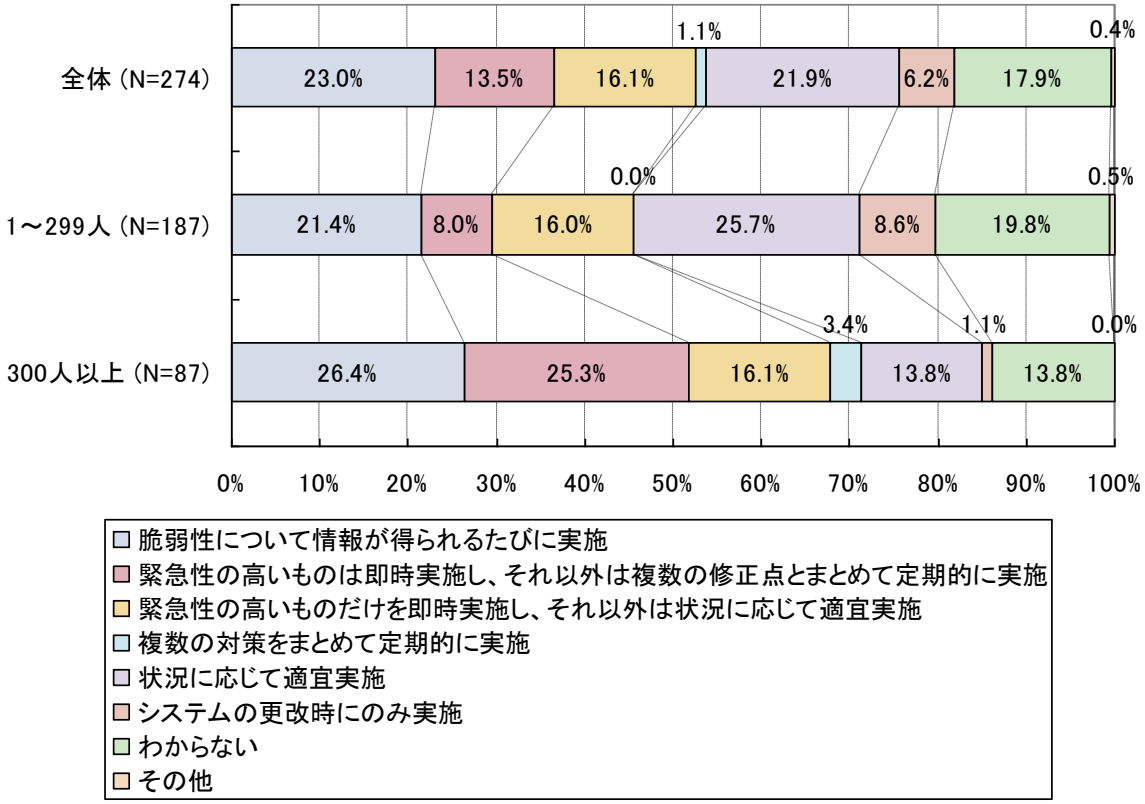

図 3.4-16　ウェブサイトの脆弱性を修正するタイミング（規模別）

3.4.14. 脆弱性対策に関する費用・人員の確保状況

ウェブサイトの脆弱性対策に必要な費用や人員はどの程度確保されているかを尋ねた。回答者全体では「十分に確保できている」（9.9%）、「おおむね確保できている」（30.7%）の回答を合わせ、4 割ほどから費用・人員は確保されているとの回答が得られた。不足とする回答も 4 割強で、ほぼ同数であった。

組織の規模別に見ると、大企業等では、「おおむね確保できている」とする回答が 47.1%と多く、「十分に確保できている」（10.3%）と合わせると過半数に達した。

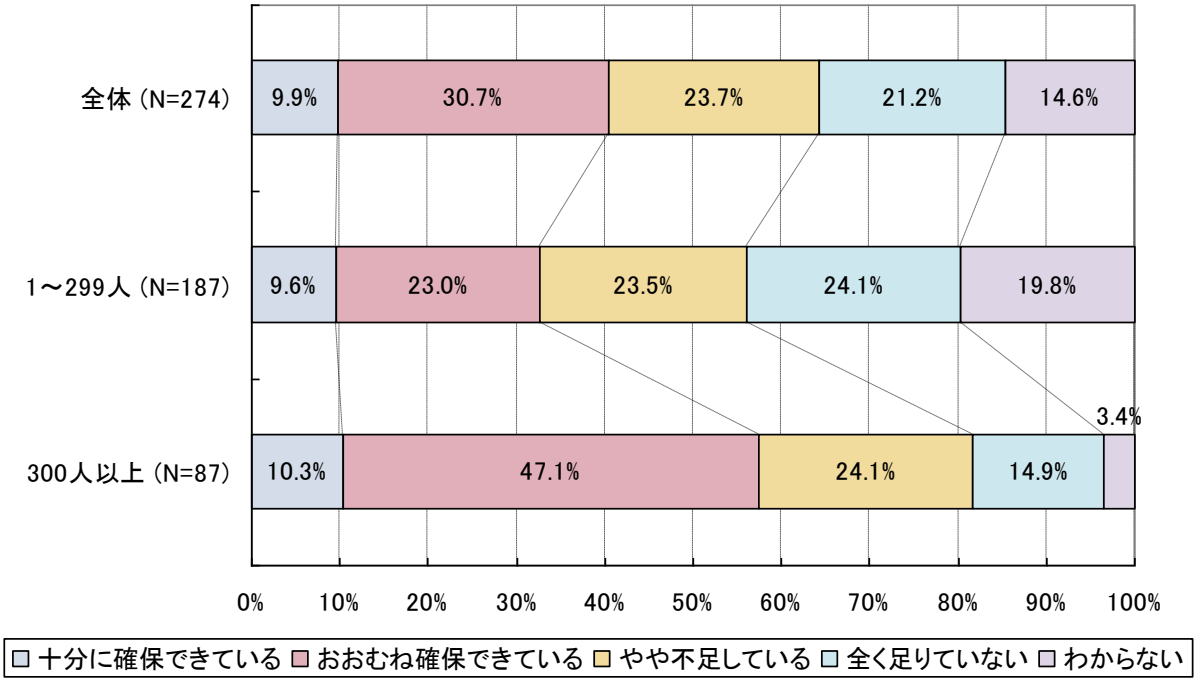

図 3.4-17　ウェブサイト脆弱性対策に関する費用・人員の確保状況

3.5. 組織内向けシステムの脆弱性対策に関する状況

3.5.1. 構築の状況

組織内向けシステムをどのように開発・構築しているかを尋ねたところ、「基本的に自組織で構築している」組織は 6 割程であり、外部事業者に委託している組織は 3 割程であった。また、大企業等のほうが外部委託する割合がやや高い。

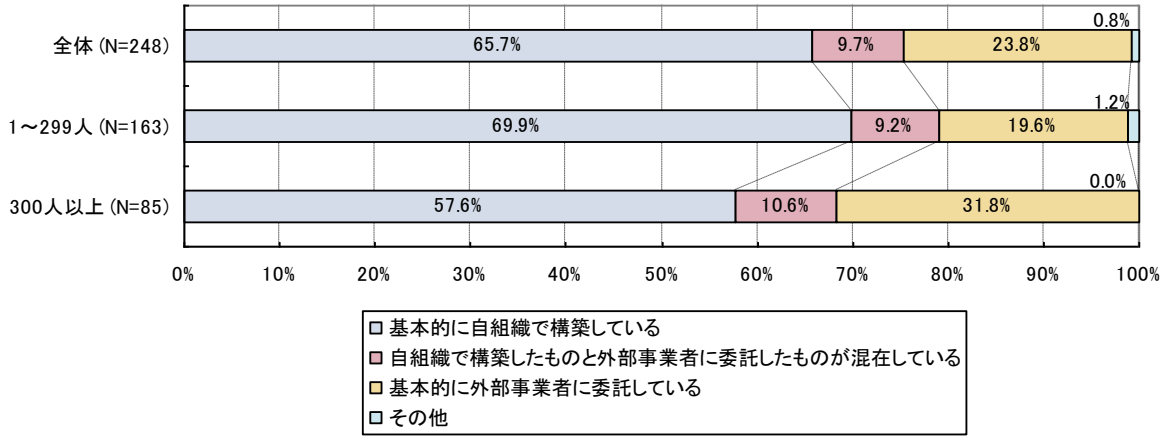

図 3.5-1　組織内向けシステムの構築状況（規模別）

3.5.2. 運用・保守の状況

自組織で運用・保守しているという回答が 7 割ほどであった。外部事業者に運用・保守を委託している企業はおよそ 3 割であった。また、大企業等のほうが外部委託する割合が高い。

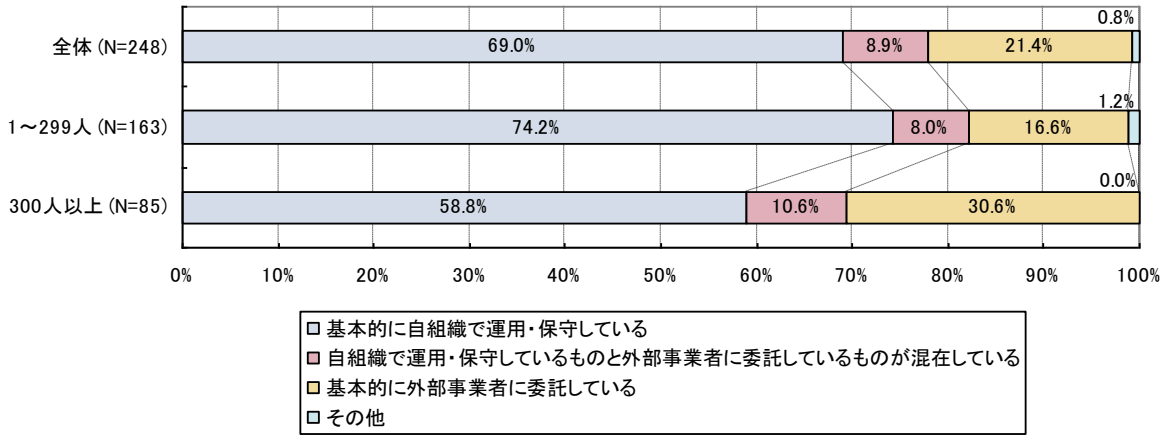

図 3.5-2　組織内向けシステムの運用・保守状況（規模別）

3.5.3. 構築時の対策の状況

組織内向けシステム構築時に脆弱性対策をどのように行っているかを尋ねた。構築の時点で脆弱性対策を行っている組織は大企業等で 65.9%あるのに対し、中小企業等では 44.2%にとどまる。

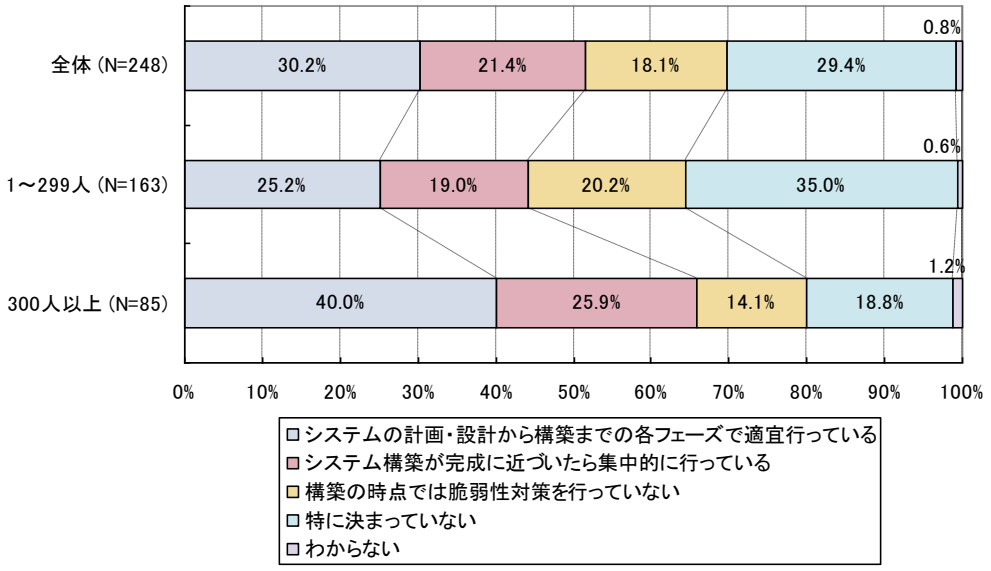

図 3.5-3　組織内向けシステム構築時の脆弱性対策の状況（規模別）

3.5.4. 運用中の脆弱性検査・診断サービスの利用状況

運用中の組織内向けシステムへの脆弱性検査等は、自組織内の検査と外部サービス利用を合わせると全体では 5 割超、大企業等での実施率は 7 割を超えている。

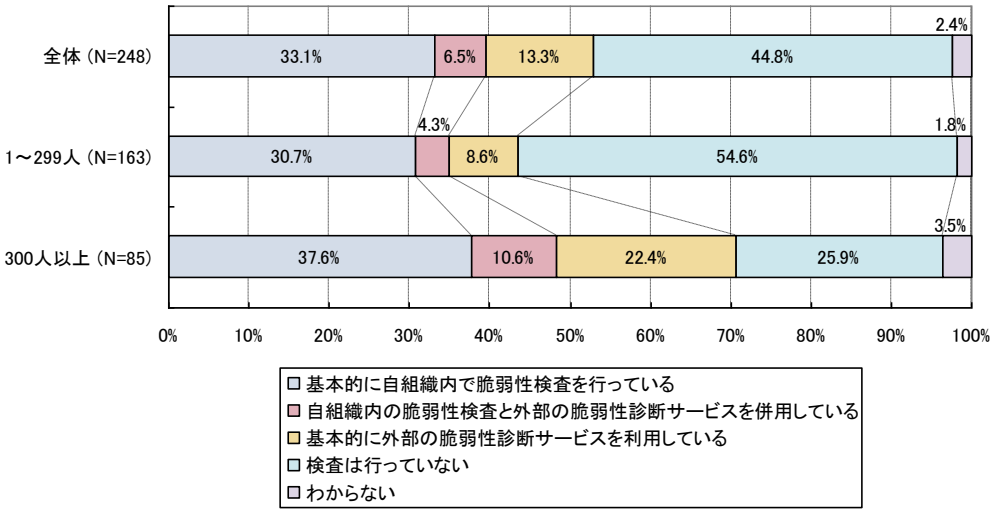

図 3.5-4　組織内向けシステム運用中の脆弱性検査・診断サービスの利用状況

3.5.5. 脆弱性に気付くきっかけ

組織内向けシステムの脆弱性について気付くきっかけとしては、大企業等では「脆弱性に関する情報を入手して確認したところ気付いた」(50.6%)、「脆弱性検査や脆弱性診断サービスによって気付いた」(40.0%) という回答が特に多かった。主体的・能動的にセキュリティ対策を進める上で気付くケースが多いことがうかがえる。また、中小企業等では「意識的に脆弱性対策を実施したことはない」とする回答をした組織が 34.4%と大企業等 (16.5%) に比べ高い比率を示した。

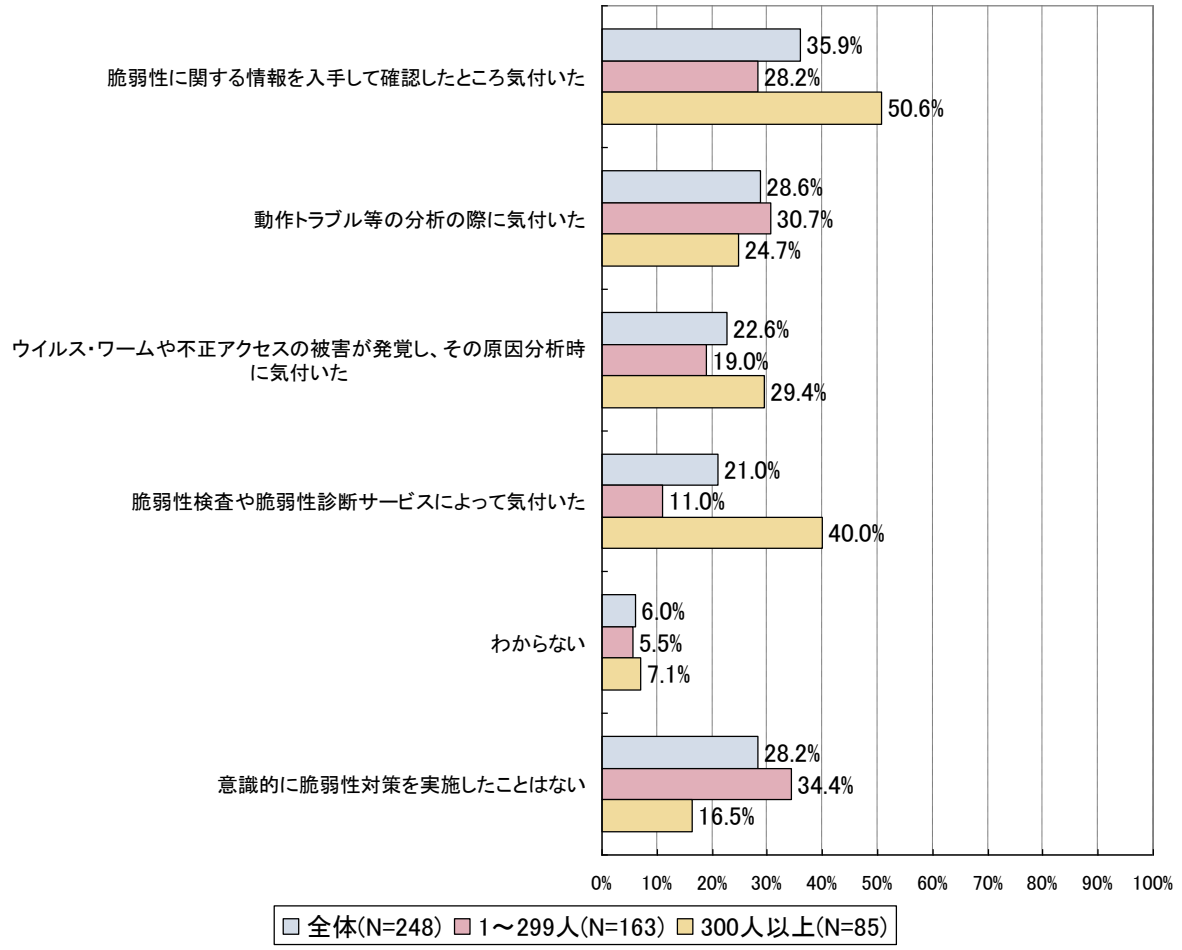

図 3.5-5　組織内向けシステムの脆弱性に気付くきっかけ（規模別）

3.5.6. 脆弱性対策の判断時に参考とする情報

組織内向けシステムの脆弱性対策の判断に際しては、「セキュリティ関連製品・サービスベンダが示す脅威レベルの評価」を挙げる組織が最も多く（45.2%）、次いで「ソフトウェア製品のメーカが提供する脅威および修正適用に伴う影響の情報」（41.1%）が挙げられた。この点については組織の規模による差異は殆ど見られなかった。

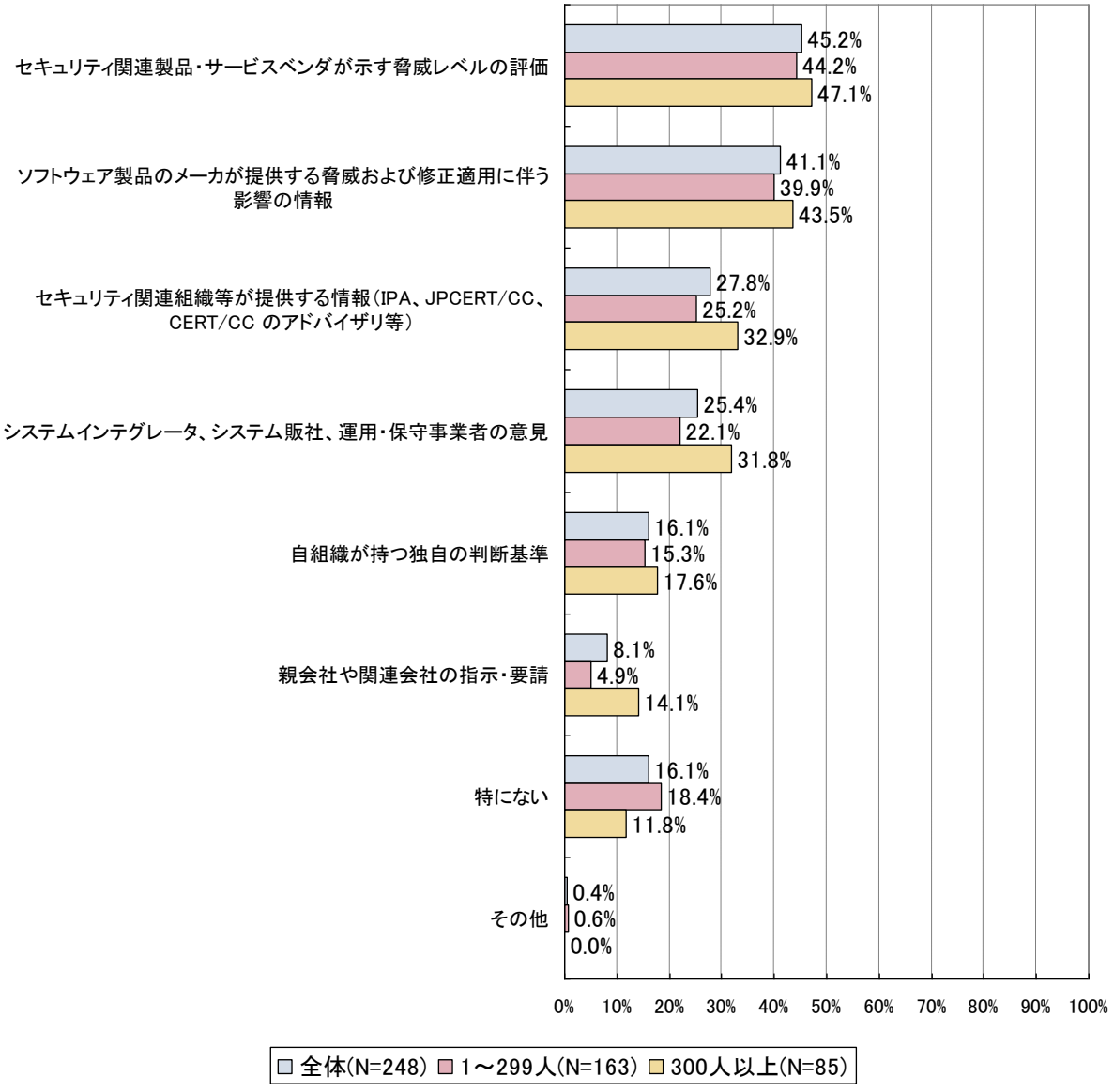

図 3.5-6　組織内システムの脆弱性対策の判断時に参考とする情報（規模別）

3.5.7. 脆弱性対策の適用を判断する人

「情報セキュリティ管理の担当部署の責任者」を挙げる回答が最も多く、全体の約 4 割を占めた。この傾向は中小企業等と大企業等での差異があまりなく、組織内向けシステムに関しては中小企業等においてもセキュリティ担当者を定めて組織的に対処している様子が伺える。

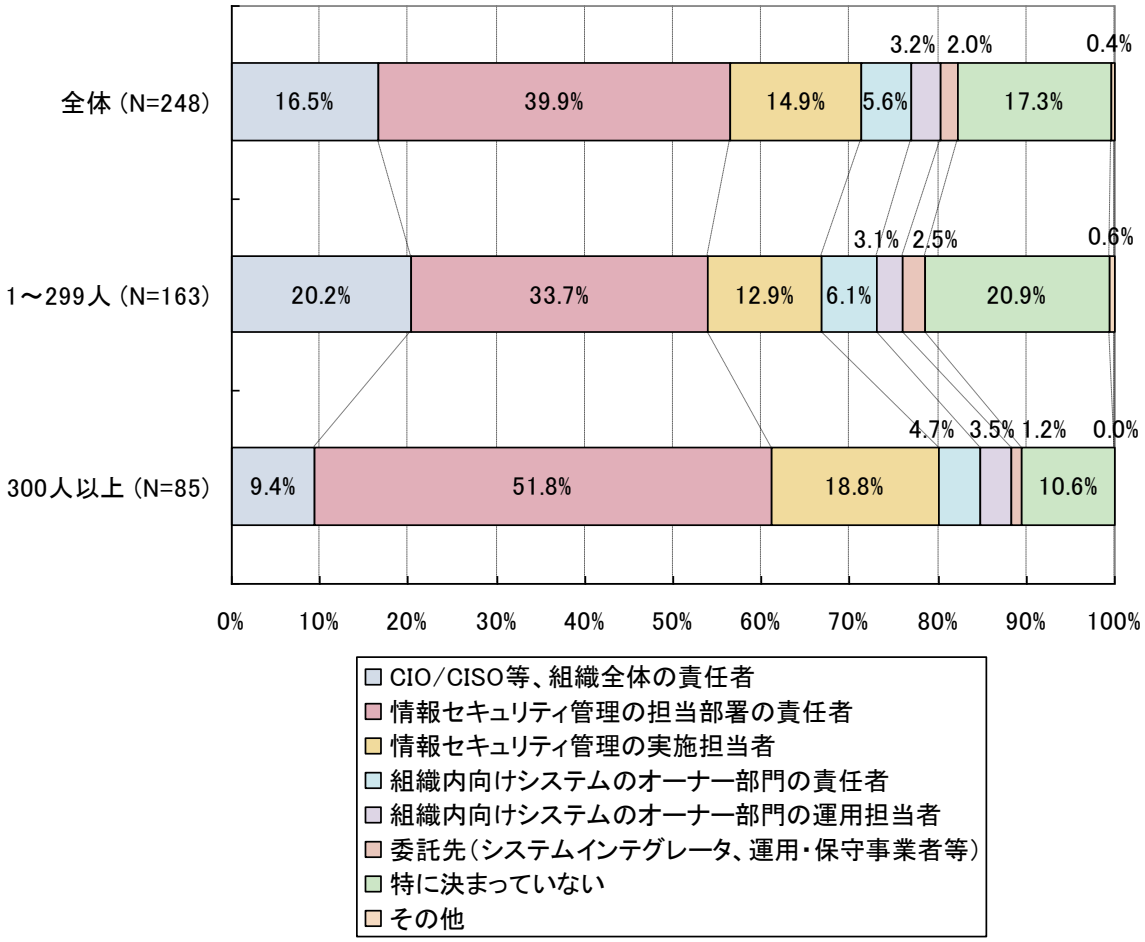

図 3.5-7　組織内向けシステムの脆弱性対策の適用を判断する人（規模別）

3.5.8. 組織内向けシステム脆弱性対処手順の文書化状況

組織内向けシステムに関する脆弱性情報の収集、脆弱な箇所の特定と報告、対処方針の決定、対策実施といった一連の手順を文書化しているかを尋ねた。大企業等においては対処手順を47.1%の組織が「組織内ルールとして文書化」しているが、中小企業等においては14.1%に留まった。中小企業等においてはおよそ7割の組織が「特に定まった手順はない」としている。

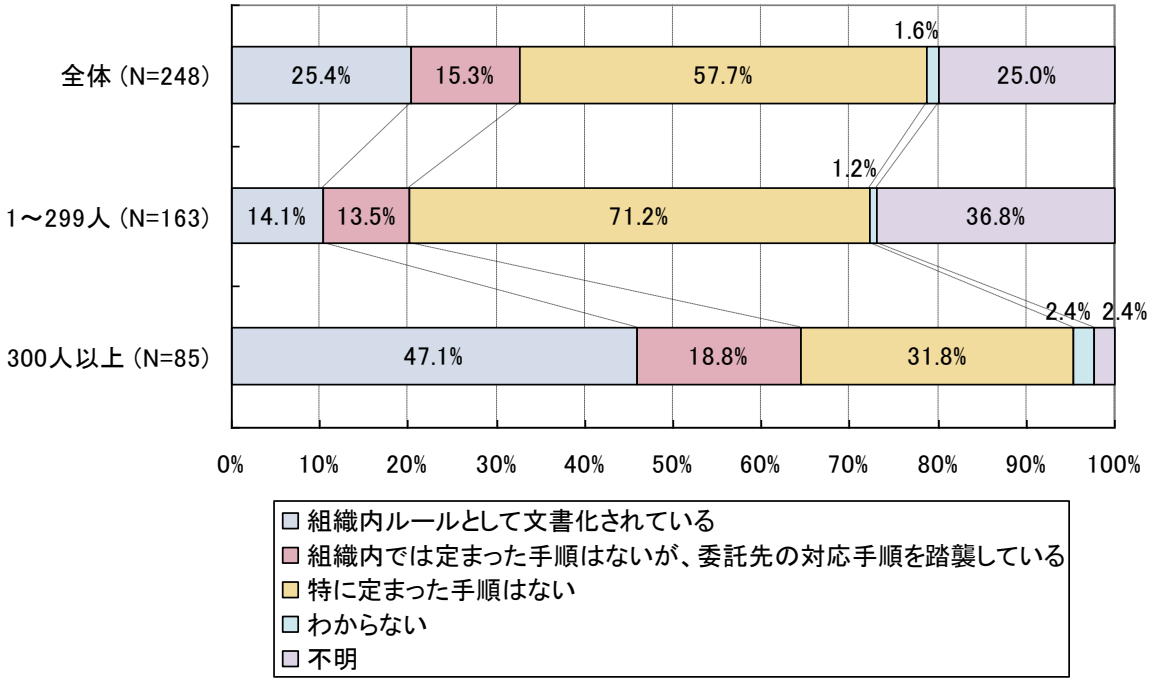

図 3.5-8 組織内向けシステムの脆弱性対処手順の整備（規模別）

3.5.9. 組織内向けシステムの被害経験

組織内向けシステムの脆弱性対策における遅れやミスが間接的な原因となって、不正アクセス等の被害に遭った経験は、中小企業等では 23.3%にとどまるのに対し、大企業等では 53.0%に達し、その半分以上は「複数部門の業務に影響が生じる被害が発生した」経験を有する。

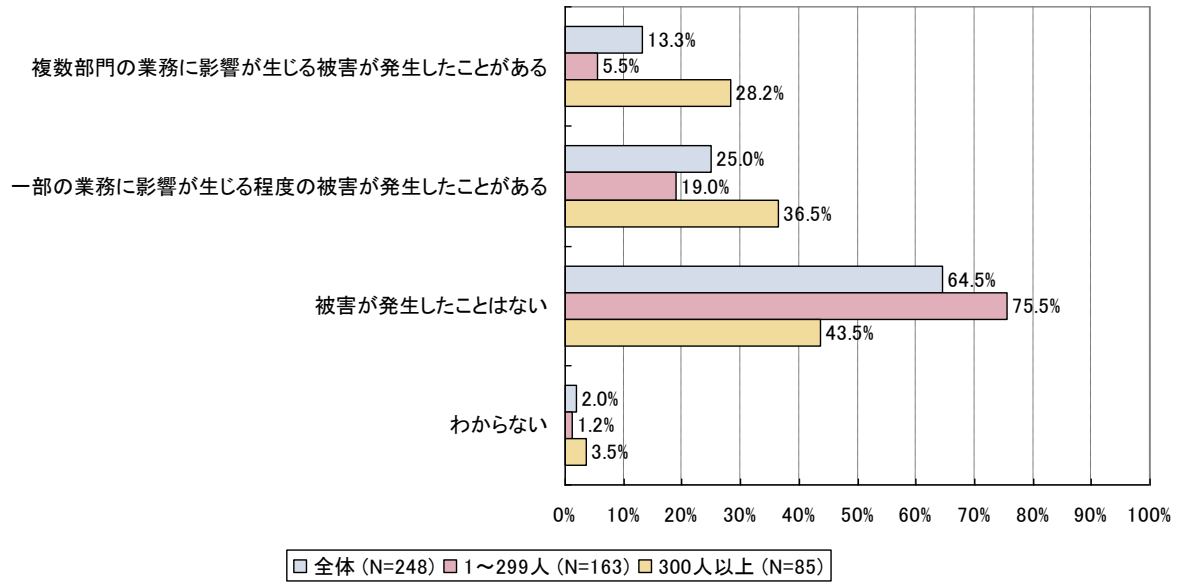

図 3.5-9　組織内向けシステムの脆弱性が関係する不正アクセス等の被害の経験（規模別）

3.5.10. 修正適用の作業担当者

「情報セキュリティ管理の実施担当者」という回答が 7 割弱を占め、この結果については組織の規模による差異は殆ど見られなかった。

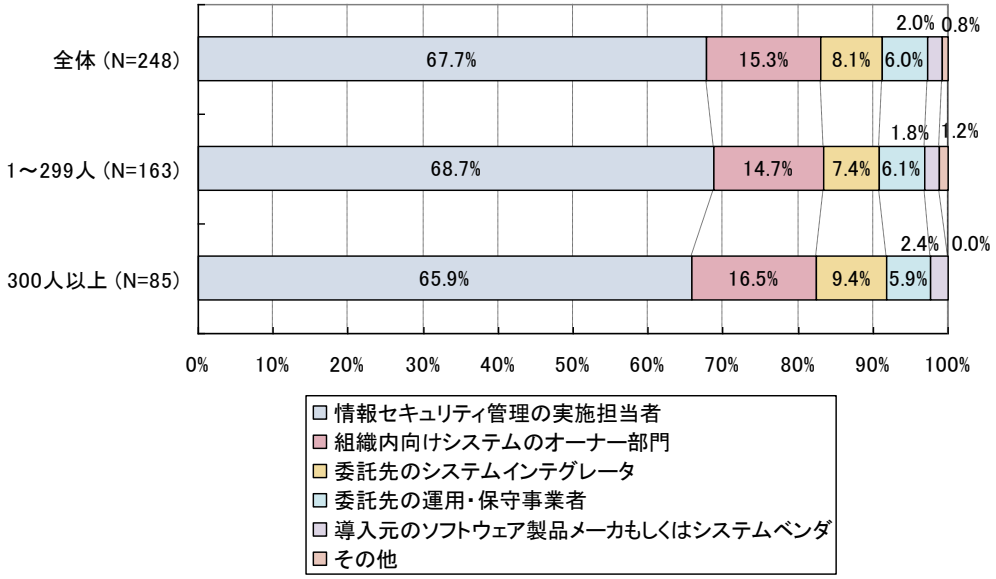

図 3.5-10　組織内向けシステムの修正適用の作業担当者（規模別）

先の設問で「委託先のシステムインテグレータ」、「委託先の運用・保守事業者」、「導入元のソフトウェア製品メーカもしくはシステムベンダ」、「その他」と答えた回答者に対して、組織内向けシステムにおける脆弱性対策の費用負担と委託契約の状況について尋ねた。

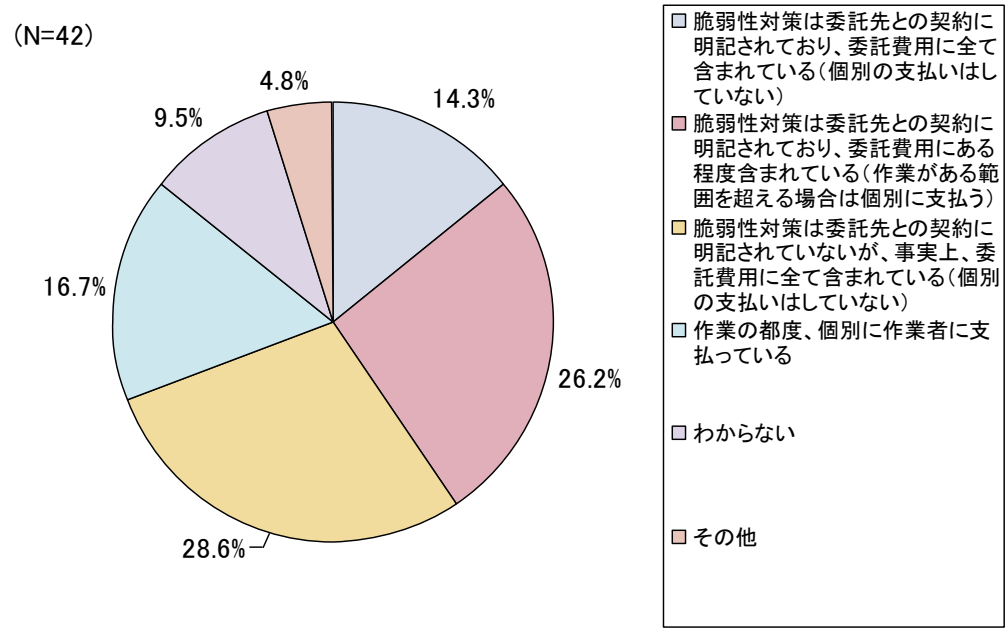

図 3.5-11　組織内向けシステムの脆弱性対策に関する委託契約と費用負担

3.5.11. 組織内向けシステム脆弱性修正タイミング

「緊急性の高いものは即時実施し、それ以外はまとめて定期的に実施」を選択した組織は、中小企業等では 13.5%であったのに対し、大企業等では 31.8%であった。また、「状況に応じて適宜実施」を選択した組織は、中小企業等では 29.4%であり、大企業等では 14.1%であった。組織の規模が大きな企業等では脆弱性対策をより計画的に実施している様子が伺える。

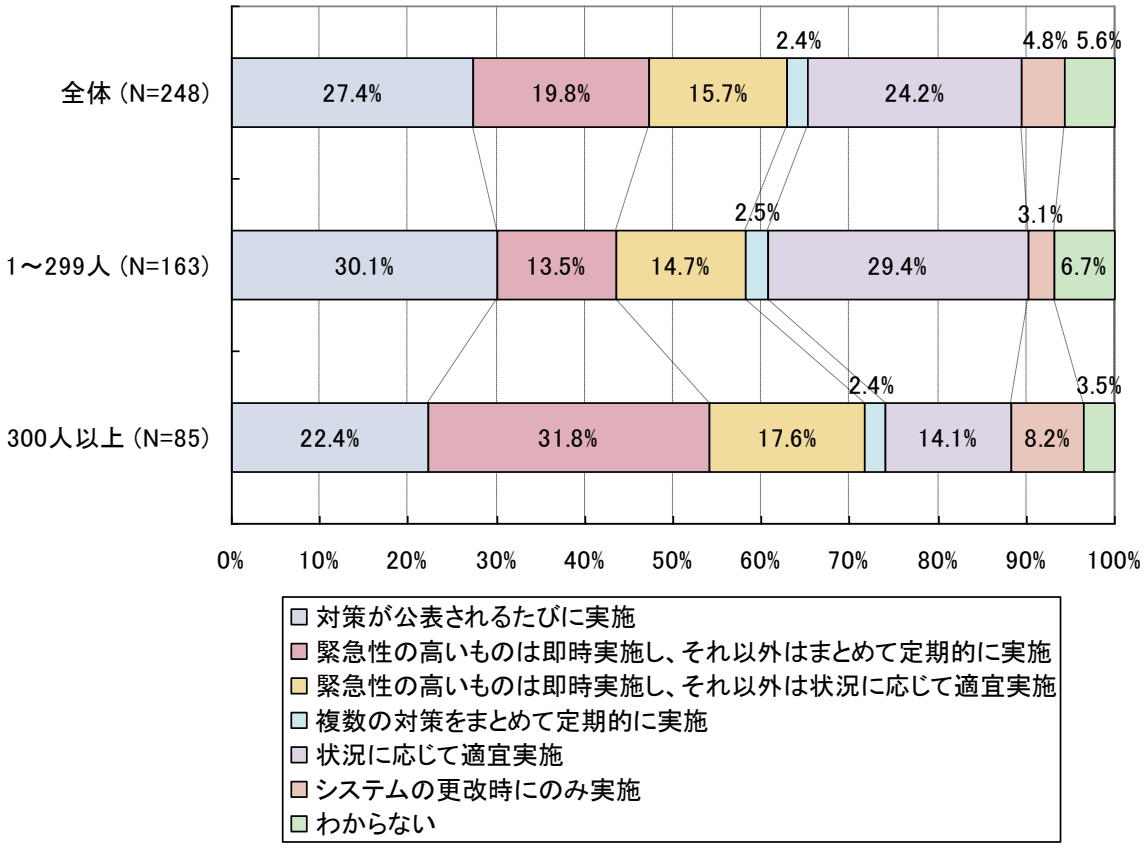

図 3.5-12　組織内向けシステムにおける脆弱性修正のタイミング（規模別）

3.5.12. 脆弱性対策費用・人員の確保の状況

組織内向けシステムの脆弱性対策に必要な費用や人員はどの程度まで確保されているかを尋ねた。全体では「十分に確保できている」または「おおむね確保できている」と回答した組織は 45.6%、「やや不足している」または「全く足りていない」と回答した組織は 49.6%であり、確保できているとする組織と、できていないとする組織はほぼ同数であった。

組織の従業員数規模別に見ると、確保できていないとする回答は中小企業等においては 55.2%、大企業等においては 38.8%であり差異が生じていた。中小企業等においてセキュリティ担当者あたりの業務負担が大きいこと、セキュリティ以外の業務も担当する者がセキュリティ対策に携わっていることなどが背景にあると考えられる。

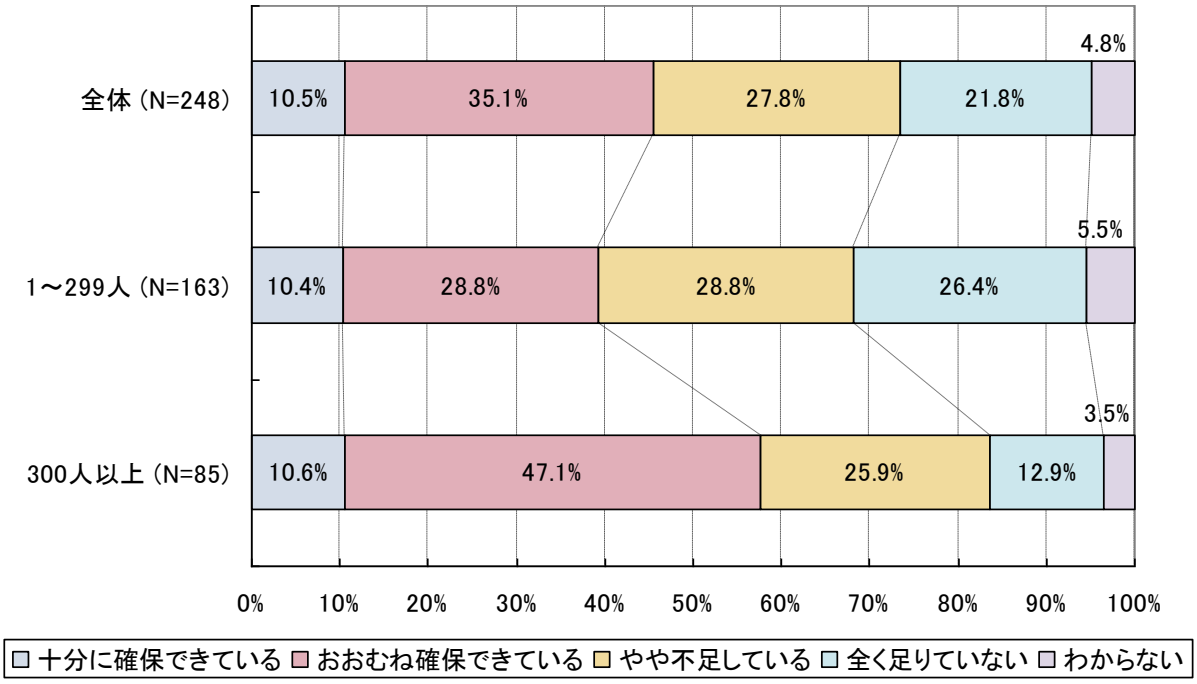

図 3.5-13　組織内向けシステムにおける脆弱性対策費用・人員の確保の状況（規模別）

3.6. クライアント PC の脆弱性対策に関する状況

3.6.1. 導入時の脆弱性対策の実施状況

従業員のクライアント PC を導入する際に、ソフトウェアの脆弱性の検査や修正などの対策は実施しているかを尋ねた。「特に対策はしていない」との回答は全体の 23.5%にとどまり、8 割近くの組織においては PC 導入時に何らかの脆弱性対策が行われている。

規模別に見ると、大企業等では「特に対策はしていない」とする回答は 15.1%と少なく、「導入時に委託先が対策を施している」とする回答が 29.1%と高い比率を示した。規模の大きな組織では組織的に導入時の対策を行っている様子が伺える。

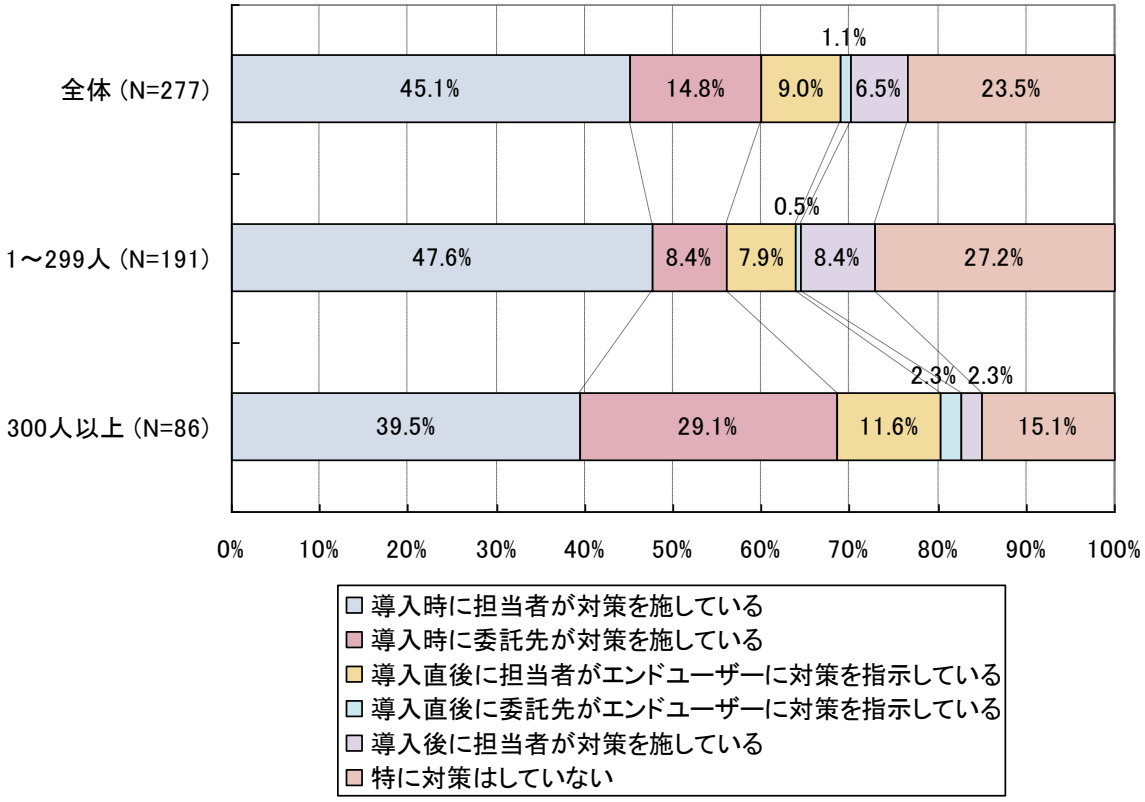

図 3.6-1　クライアント PC 導入時の脆弱性対策の実施状況（規模別）

3.6.2. 運用時の脆弱性対策の実施状況

クライアント PC を導入した後の運用段階において、エンドユーザーの PC のソフトウェアに関する脆弱性対策を誰がどのように実施しているかを尋ねた。

担当者が対策あるいは対策実施の指示をしているとする回答については中小企業等では 70.1%、大企業等では 72.1%と、ほぼ同率を示した。その内訳を見ていくと、中小企業等の 48.7%が「担当者が 1 台ずつ対策している」のに対して、大企業等の 39.5%が「担当者が統合管理ツール等を用いて複数の PC について一斉に対策して」おり、「担当者が 1 台ずつ対策している」ケースは 16.3%にとどまる。このことから、規模が大きい組織では担当者は効率的な脆弱性対策を行っている様子が伺える。

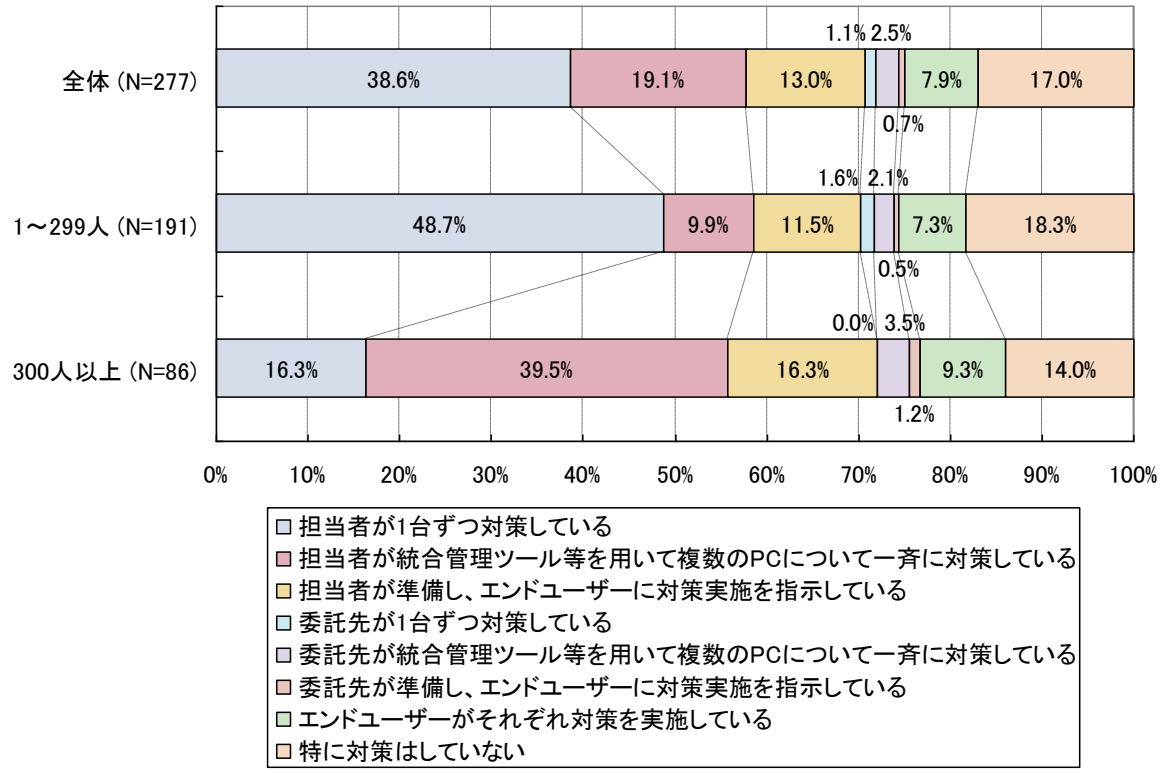

図 3.6-2　クライアント PC 運用時の脆弱性対策の実施状況

3.6.3. クライアント PC の脆弱性に基づく不正アクセス等の被害経験

クライアント PC の脆弱性対策における遅れやミスが間接的な原因となって、不正アクセス等の被害に遭った経験は、中小企業等では 19.9%にとどまるのに対し、大企業等では 59.3%に達し、その約 4 割が「複数部門の業務に影響が生じる被害が発生した」経験を有する。

この結果は、規模の大きい組織ほど、ミスをして被害に遭うユーザが発生する確率が高いことが影響したものと考えられる。

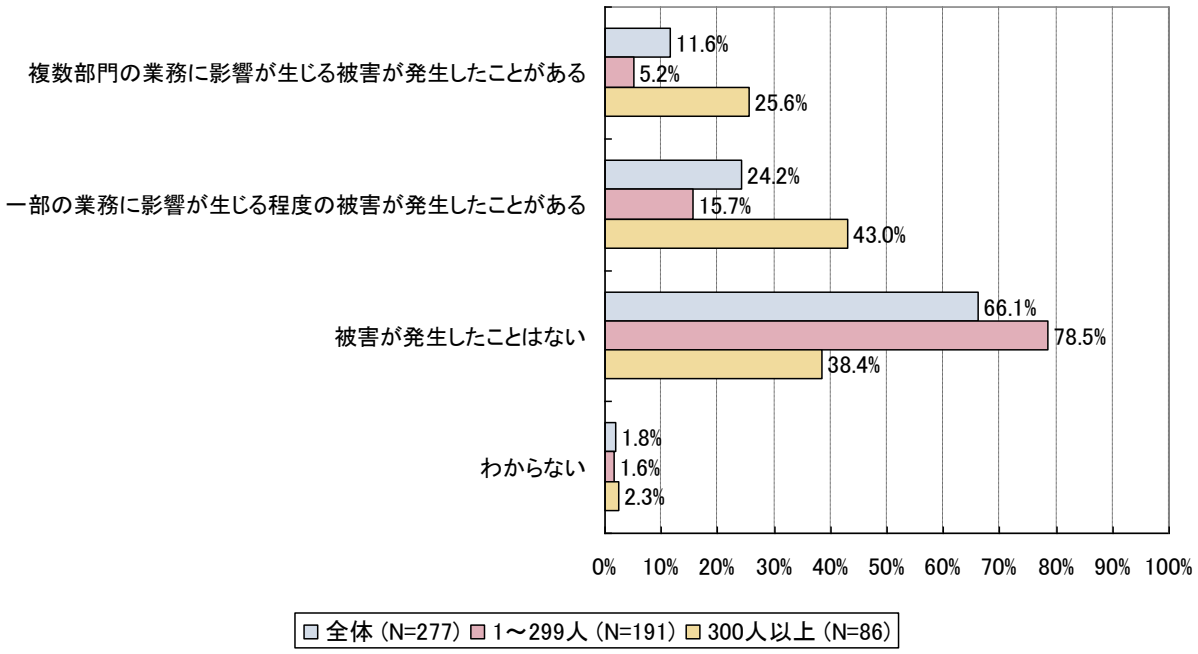

図 3.6-3　クライアント PC の脆弱性に基づく不正アクセス等の被害経験

3.6.4. クライアント PC の具体的な脆弱性対策の状況

クライアント PC のソフトウェアに関する具体的な脆弱性について組織全体として対策をしているかを尋ねた。いずれの脆弱性についても、おおよそ 6 割の組織では「対策済み」、1.5 割ほどの組織では「対策を検討・実施中」であった。

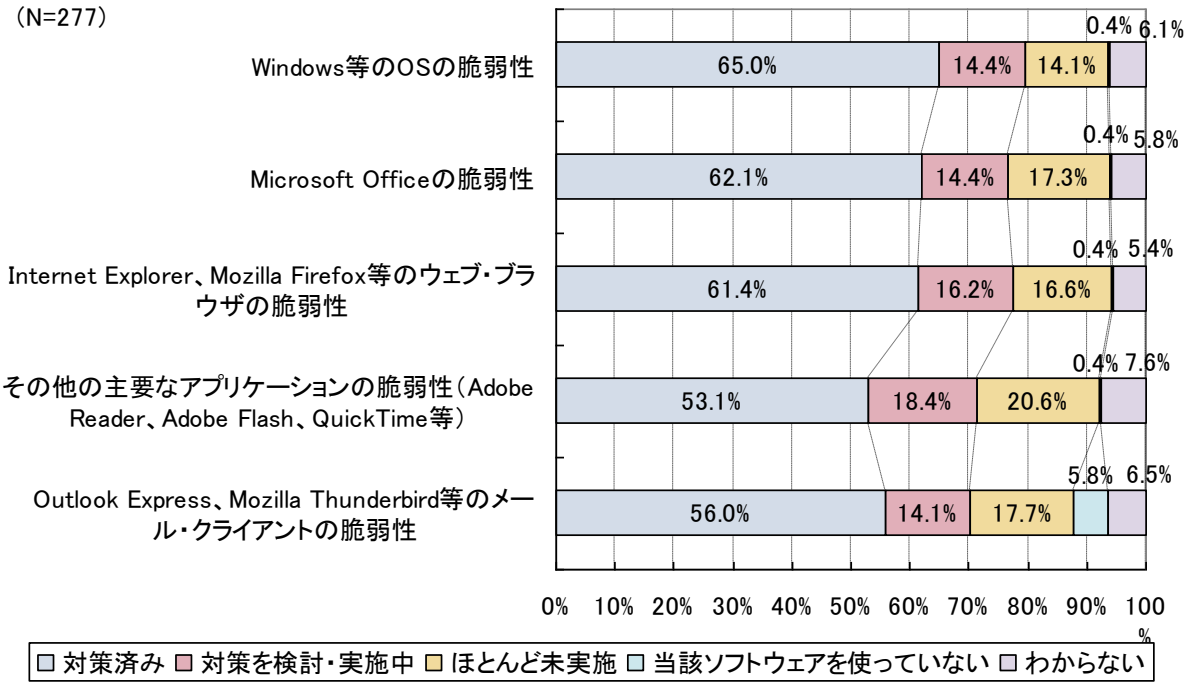

図 3.6-4　クライアント PC の具体的な脆弱性対策の状況

3.7. 脆弱性対策に関する課題

3.7.1. 脆弱性対策を推進する目的

回答者全体では「情報セキュリティ上のリスクを低減するため」（69.4%）が最も多く、次いで「組織としての信頼感や競争力を高めるため」（38.1%）が続いた。この傾向は組織の規模に係らず同様であったが、特に大企業等においては「組織としての信頼感や競争力を高めるため」とする回答が中小企業等に比べ多くみられた。

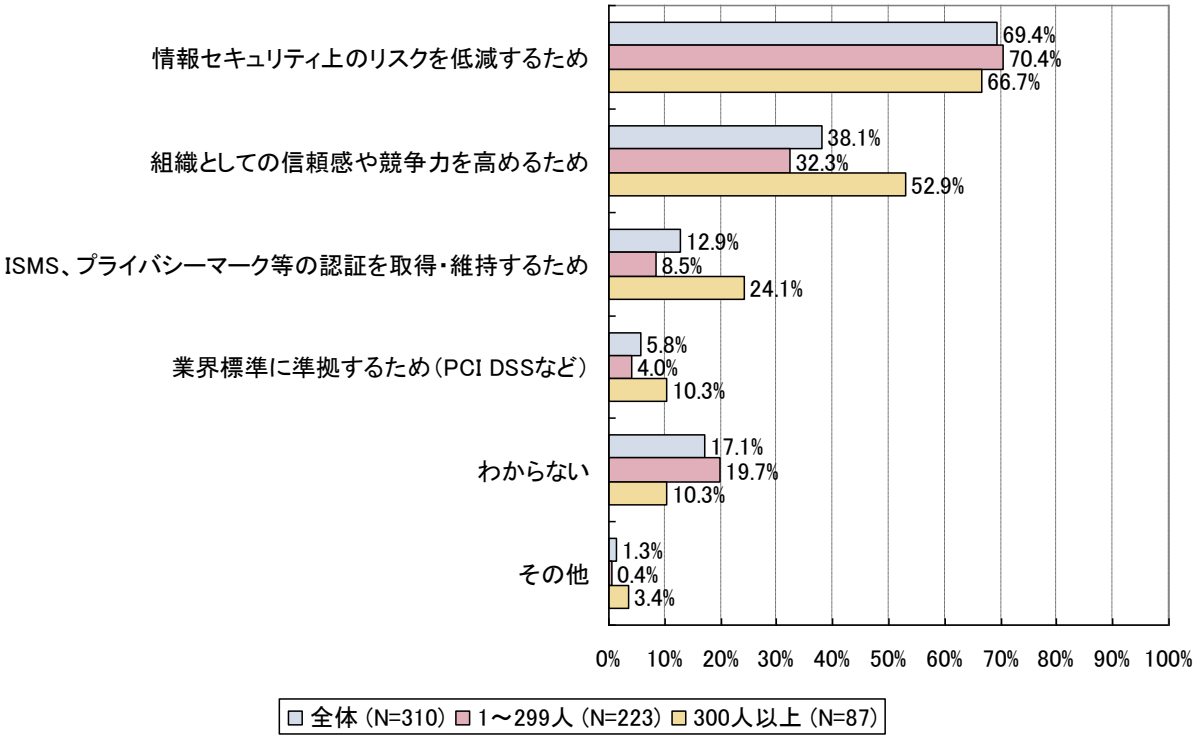

図 3.7-1　脆弱性対策を推進する目的（規模別）

3.7.2. 脆弱性対策を始めたきっかけ

回答者全体では「脆弱性を狙う攻撃が流行していると聞いて」対策を始めるケースが 33.2%と最も多かった。また、「明確なきっかけは無く、脆弱性対策は常日頃から行っている」とする回答は全体では 25.5%であった。

組織の規模についてみると、特に大企業等においては、「親会社・監督機関や取引先等から要望されたので」、「新たにセキュリティポリシー等を策定し具体的な対策を合わせて実施するので」、「組織の外部の人からシステムに脆弱性が存在すると知らされたので」との回答がいずれも 20%を超えており、中小企業等と比較してもきっかけとして挙げる組織の比率が高かった。

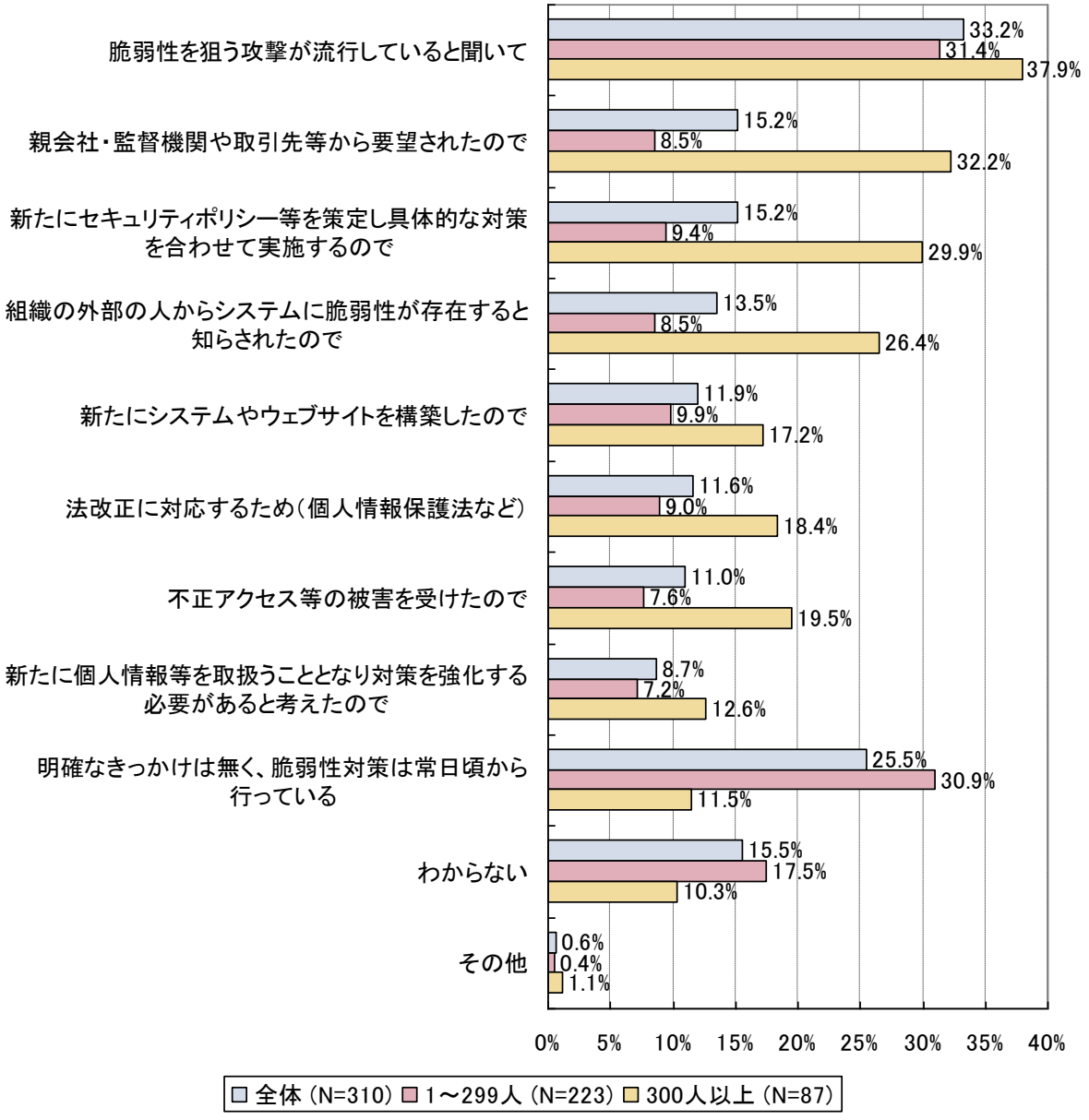

図 3.7-2　脆弱性対策をはじめたきっかけ（規模別）

3.7.3. 脆弱性対策における課題認識

脆弱性対策における課題について、複数の例を示し、それぞれについて課題としてのどの程度重要視しているかを尋ねた。

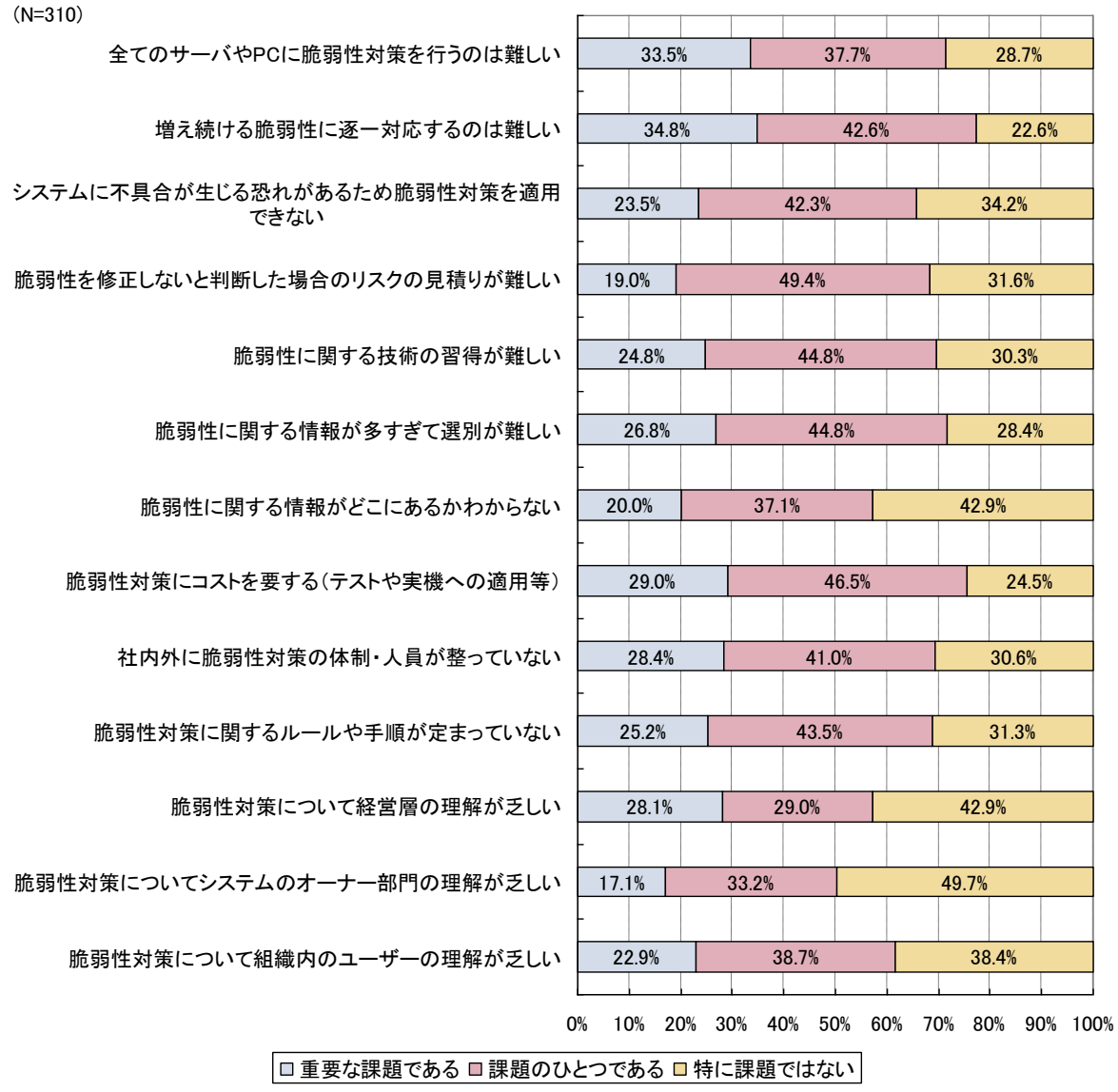

図 3.7-3　脆弱性対策における課題認識

項目「全サーバ等に脆弱性対策を行うのは難しい」については、サーバが少ない中小企業等においては特に課題とは捉えておらず（36.3%）、逆に大企業等では重要な課題と捉えている（50.6%）傾向が捉えられた。

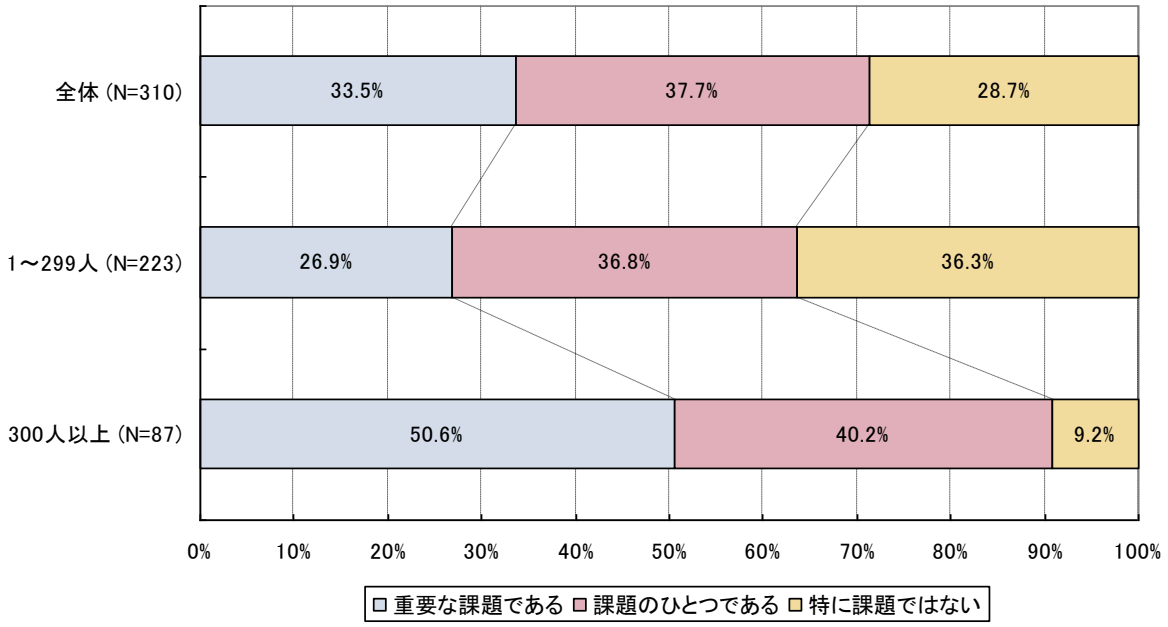

図 3.7-4　課題認識 ― 全てのサーバや PC に脆弱性対策を行うのは難しい（規模別）

「脆弱性対策について経営層の理解が乏しい」「脆弱性対策についてシステムオーナー部門の理解が乏しい」の項目については、中小企業等ではいずれも「特に重要な課題ではない」とする回答が多かった。これは中小企業等においては、セキュリティ担当者と経営者・システムオーナー部門との密な連絡が可能であることが伺える。

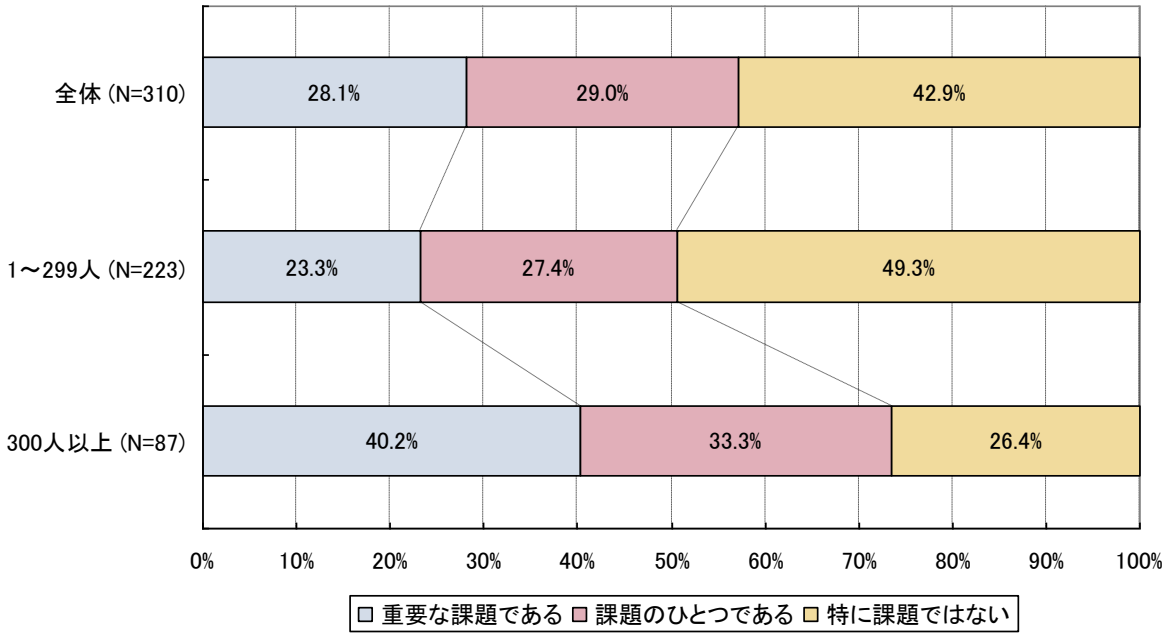

図 3.7-5　課題認識 ― 脆弱性対策について経営層の理解が乏しい（規模別）

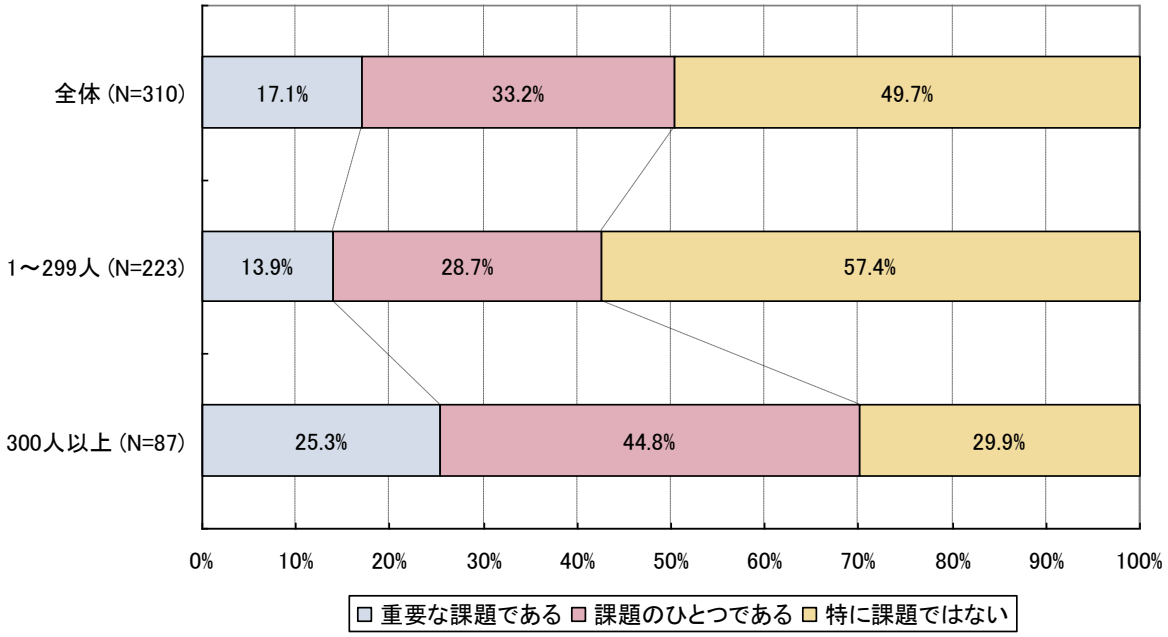

図 3.7-6　課題認識 ― 脆弱性対策についてシステムのオーナー部門の理解が乏しい（規模別）

4. 考察

4.1. 脆弱性対策の整備状況に基づく分析

- 組織規模により脆弱性対策の取り組みに格差が見られた。大企業等は体制や手順を整え、WAF や統合管理ツール等も導入し、JVN 等の情報も有効に活用しているのに対し、中小企業等は被害経験が乏しく、対策の必要性を強く感じていないものと考えられる。
- ウェブサイトに対する脆弱性検査や脆弱性診断サービスは、大企業等で約 8 割、中小企業等でも約 4 割が実施しており、一般化しつつあるといえる。
- 組織内向けシステムに比べウェブサイトにおける脆弱性対策が遅れている傾向が見られた。これはウェブサイトについては現場主導の構築・運用がなされやすいため、組織的な脆弱性対策の意識付けが乏しいと推測される。ウェブサイトに外部から攻撃を受けるリスクが高いことを踏まえれば、手厚い脆弱性対策を施すことが望まれる。
- WAF は、今回の調査対象となった大企業等の約半分、中小企業等の約 1/4 が活用しており、ウェブサイトの脆弱性対策において一定の役割を担っている様子が伺える。しかし、WAF を利用している組織の 1/3 が「ウェブアプリケーションの修正を行わない」とも回答しており、根本的な脆弱性の解消を伴わない利用がなされていない状況が伺える。
- クライアント PC の脆弱性対策において、統合管理ツールは大企業等の約 4 割が活用している一方、中小企業等の活用は 1 割に満たない。このことから、統合管理ツールは、規模の負担を軽減するツールとしてのポジションを確立していることが伺える。

- 以下では、「脆弱性対策が進んでいる企業」と「これから脆弱性対策に取り組む企業」のそれぞれについての特徴を抽出した。いくつかの設問の解答を軸にして回答者をグループ分けし、他の設問への解答状況をみている。

「ウェブサイトにおける脆弱性対策の手順化の状況」により回答者を 2 グループに分け「ウェブサイトにおける被害経験」の有無についてみる。

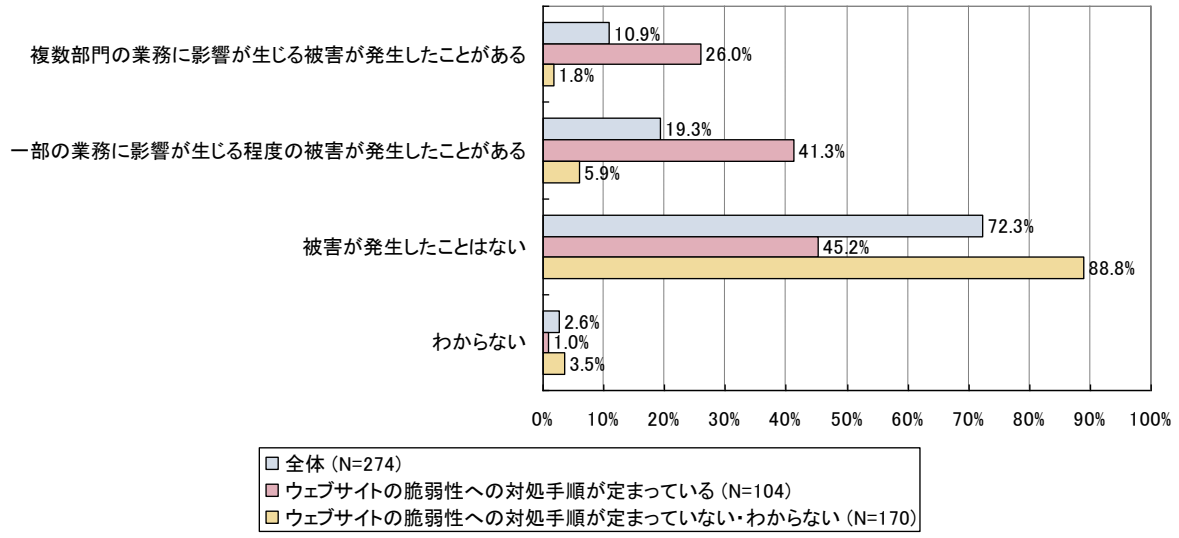

図 4.1-1　ウェブサイト不正アクセス被害経験（ウェブサイト脆弱性対処手順の文書化状況別）

脆弱性対処手順の整備が進んでいる組織では被害を認識しており、手順の整備に今後取り組もうとする組織においては被害経験が少ないという傾向がみられた。被害の認識と対策の進展には相関があることが伺える。

「ウェブサイトにおける脆弱性対策の手順化の状況」により回答者を 2 グループに分け「ウェブサイトの脆弱性対策に必要な費用や人員の確保状況」について回答状況を見た。

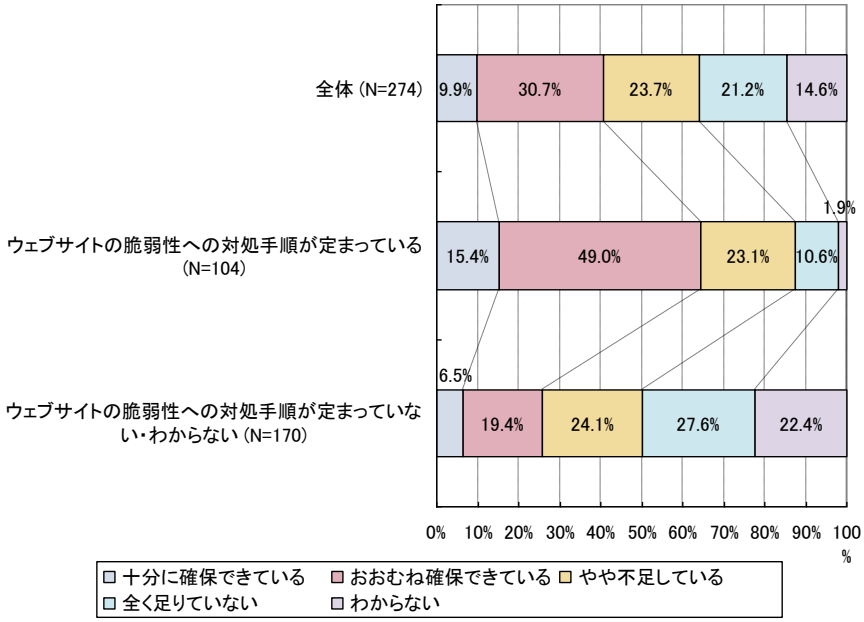

図 4.1-2　脆弱性対策費用・人員の確保状況（ウェブサイト脆弱性対処手順の文書化状況別）

脆弱性対策の手順化が進んでいる組織では費用や人員を「十分に確保できている」（15.4%）、

「おおむね確保できている」(49.0%) をあげる率が対策の手順化を進めていない組織 (6.5% および 19.4%) に比べ非常に高い。また、対策の手順化を進めていない組織では「全く足りていない」を挙げる率も 27.6%と高かった。

また、「ウェブサイト構築時の脆弱性検査や修正の状況」により回答者を 2 グループに分けて、同じ設問についての回答状況を見たところ以下のようになった。

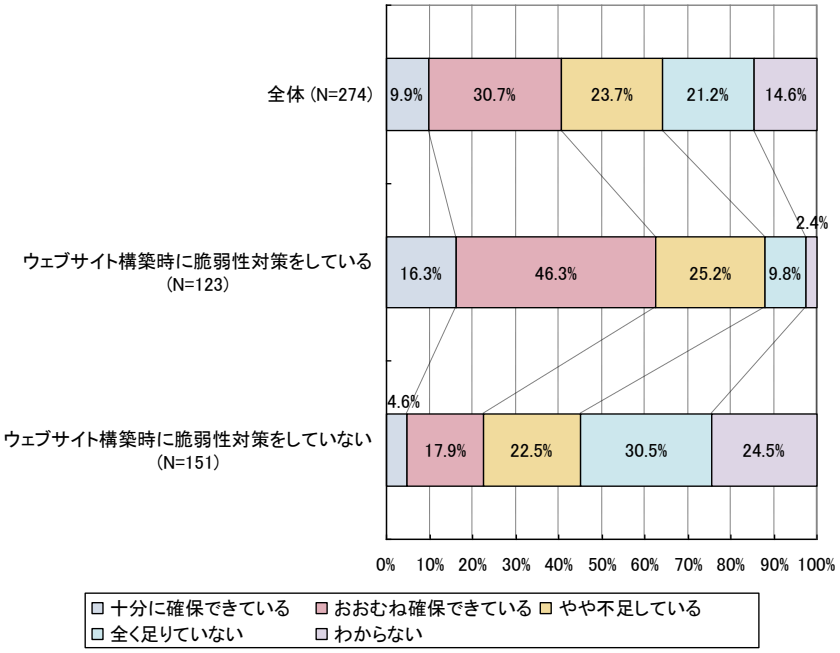

図 4.1-3　脆弱性対策費用・人員の確保状況（ウェブサイト構築時の脆弱性対策状況別）

この結果でも、脆弱性対策を構築時に行っている組織では「十分に確保できている」(16.3%)、「おおむね確保できている」(46.3%) をあげる率が、構築時に対策を進めていない組織 (4.6% および 17.9%) に比べ非常に高かった。また、構築時に対策をしていない組織では「全く足りていない」を挙げる率が 30.5%と高かった。これらの傾向は前項のグラフと類似していた。

組織内向けシステムについて「構築時に脆弱性対策を行っている組織」と「行っていない組織」とでグループ分けし、「組織内向けシステムの脆弱性対策に関する費用や人員の確保状況」を見たところ以下のような結果となっている。

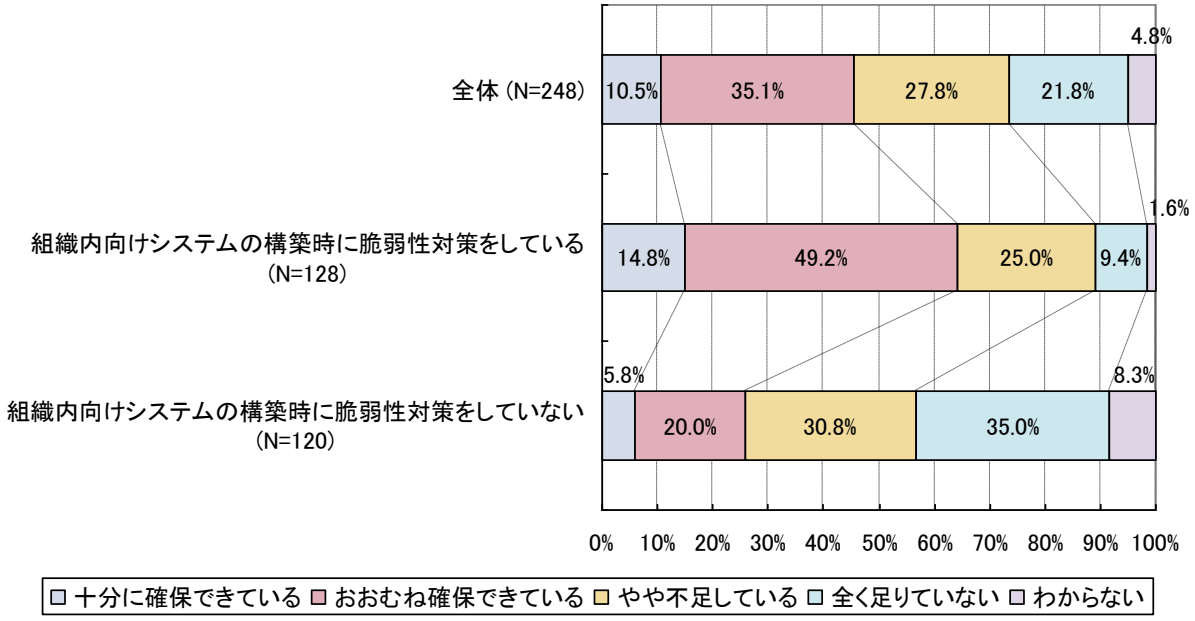

図 4.1-4　脆弱性対策費用・人員の確保状況（組織内向けシステム構築時の脆弱性対策状況別）

ここでも、脆弱性対策を構築時に行っている組織では費用や人員を「十分に確保できている」（14.8%）、「おおむね確保できている」（49.2%）とする率が、構築時に対策を進めていない組織（5.8%および 20.0%）に比べ非常に高かった。また、構築時に対策をしていない組織では「全く足りていない」を挙げる率が 35.0%と高かった。これらはウェブサイトにおける傾向と類似している。

これらの結果より、脆弱性対策の整備が既に進んでいる組織では対策費用や人員を「おおむね確保できている」のに対して、対策が未だ進んでいない組織ではこれらが「全く足りていない」とする傾向があると言えるだろう。

また、「ウェブサイトを構築時に脆弱性の検査や修正などの対策を実施しているか」で回答者を 2 グループに分け、「システムやウェブサイトにおいて脆弱性対策を始めたきっかけ」を尋ねた設問を見た。

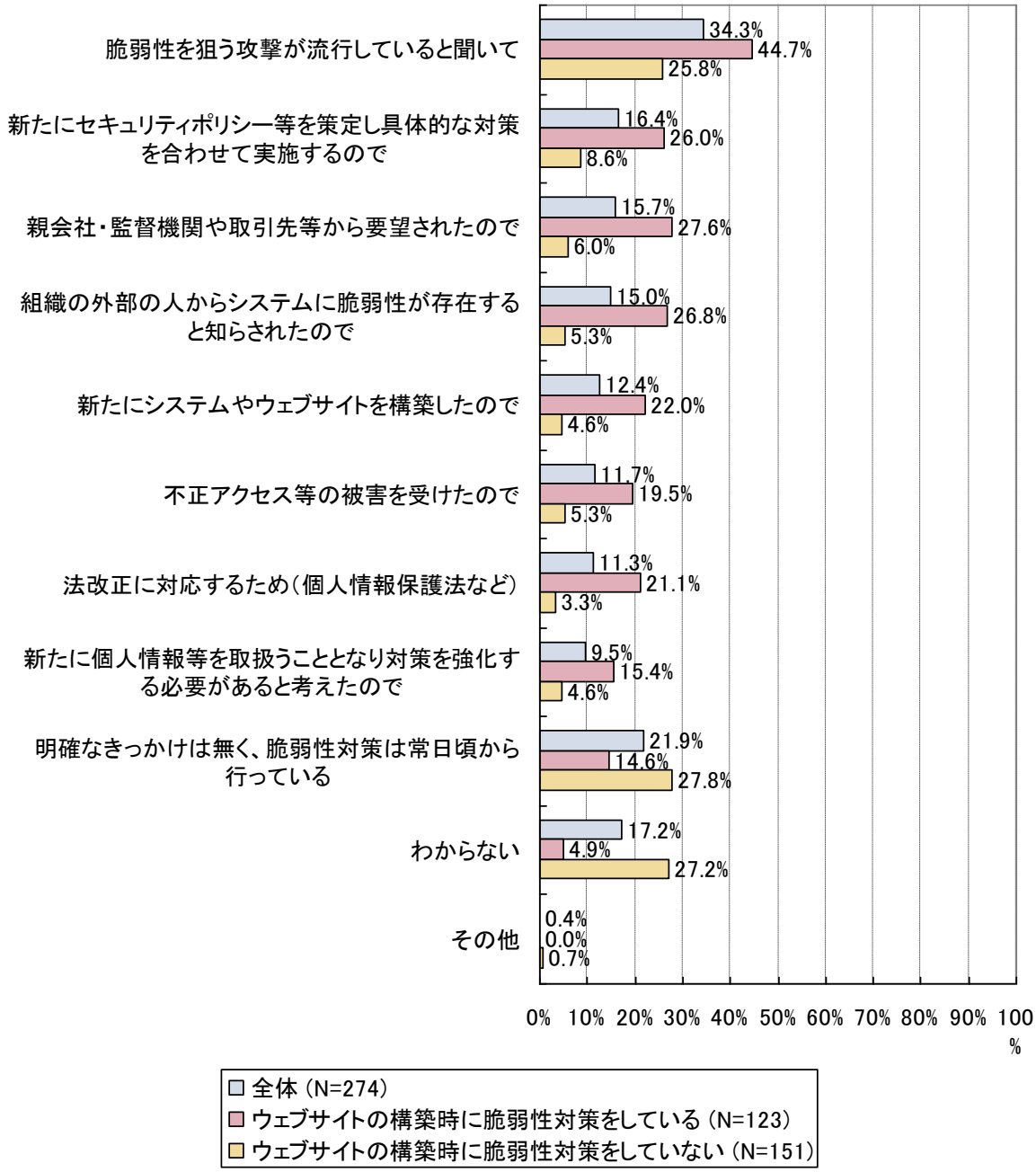

図 4.1-5　脆弱性対策を始めたきっかけ（ウェブサイト構築時の脆弱性対策状況別）

ウェブサイト構築時に脆弱性対策をしていない組織は、明確なきっかけについてはいずれも回答率が低く、「明確なきっかけがなく対策を常日頃から行っている」を選択する傾向が強く現れた。

このことから、明確なきっかけを持たずに対策を常日頃から行う方針の組織では、サイト構築時の脆弱性対策などの具体的かつ明確な対策にあまり意欲的ではない可能性が伺われる。

4.2.脆弱性対策の阻害要因

- 「増え続ける脆弱性に逐一対応するのは難しい」は「重要な課題とする」（34.8%）、「課題の一つである」（42.6%）と、最も重要かつ高い支持を集めた課題である。
- プレヒアリングにおいて指摘があった「事業を継続したいシステムのオーナー部門と脆弱性対策を行いたいセキュリティ担当者の対立」という仮説は、大企業等では「重要な課題である」（25.3%）、「課題のひとつである」（44.8%）との認識を示しており、検証できたと考えられる。ただし、中小企業等では、システム担当者（セキュリティ担当者）自身が直接管理しているケースが多いため、対立構造にならず「特に重要な課題ではない」が約 6 割という結果になったと考えられる。
- 以下では、所属する企業規模および IT 投資率に基づいて回答者を 4 グループに分け、それらの特徴をもとに脆弱性対策の阻害要因について分析を行った。企業規模については、従業員数 300 名未満および従業員数 300 名以上で分けた。また、IT 投資率については次の式に基づいて導出し、中間値が 1%であるため、1%未満および 1%以上で分けることとした。

脆弱性対策を推進する目的を尋ねる設問では各グループについて次のような結果が得られた。

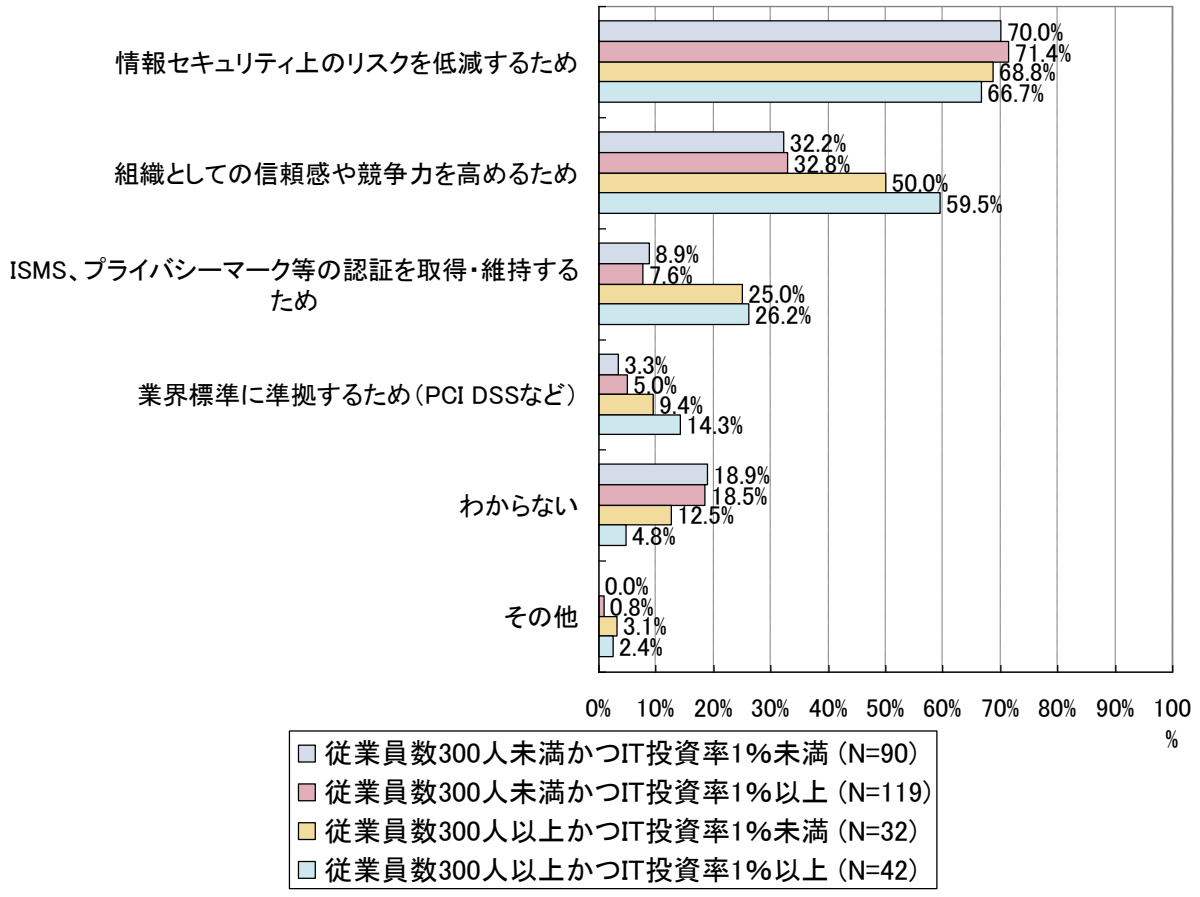

図 4.2-1　脆弱性対策を推進する目的（規模と IT 投資率別）

大企業等と中小企業等を比較すると、IT 投資の率に係らず「情報セキュリティ上のリスク

を低減するため」「組織としての信頼感や競争力を高めるため」「ISMS、プライバシーマーク等の認証を取得・維持するため」を目的に挙げる組織が多い。

脆弱性対策を始めたきっかけに関する設問では、次のような特徴が現れた（次ページ参照）。

選択肢「親会社・監督機関や取引先等から要望されたので」や「組織の外部の人からシステムに脆弱性が存在すると知らされたので」を回答する比率が中小企業等に比べ大企業等で高い（30%以上）。調査仮説を立てる時点では親会社等の要望・指摘等による対策推進が中小企業等において多いだろうと予想していたが結果はこれに反していた。大企業等の方がセキュリティ対策に関する自社周辺の社会的な状況に敏感であり、外部からの指摘も受ける機会が多いという様子が推測される。

選択肢「不正アクセス等の被害を受けたので」、「新たにシステムやウェブサイトを構築したので」、「法改正に対応するため（個人情報保護法など）」を回答する比率は、特に大企業等で IT 投資率が高い（IT 依存度が高い）組織のグループでどれも 25%以上と高く、他のグループでは 10%弱よりも低かった。これらのきっかけを、大企業等でも IT に依存しない企業では選択肢に選んでいないことから、セキュリティ対策が進展している企業においてのみ取り上げられていると考えられる。

選択肢「明確なきっかけは無く、脆弱性対策は常日頃から行っている」を挙げる比率は、特に中小企業等で IT 投資率が高い組織のグループで高く（37.8%）、次いで中小企業等で IT 投資率が低い組織のグループであった（23.3%）。このグループは、他の具体的なきっかけを挙げる比率がどれも低く、常日頃の対策を進めているとする組織では実は明確な／具体的な対策はあまり進めていないのではという疑いが持たれる結果であった。

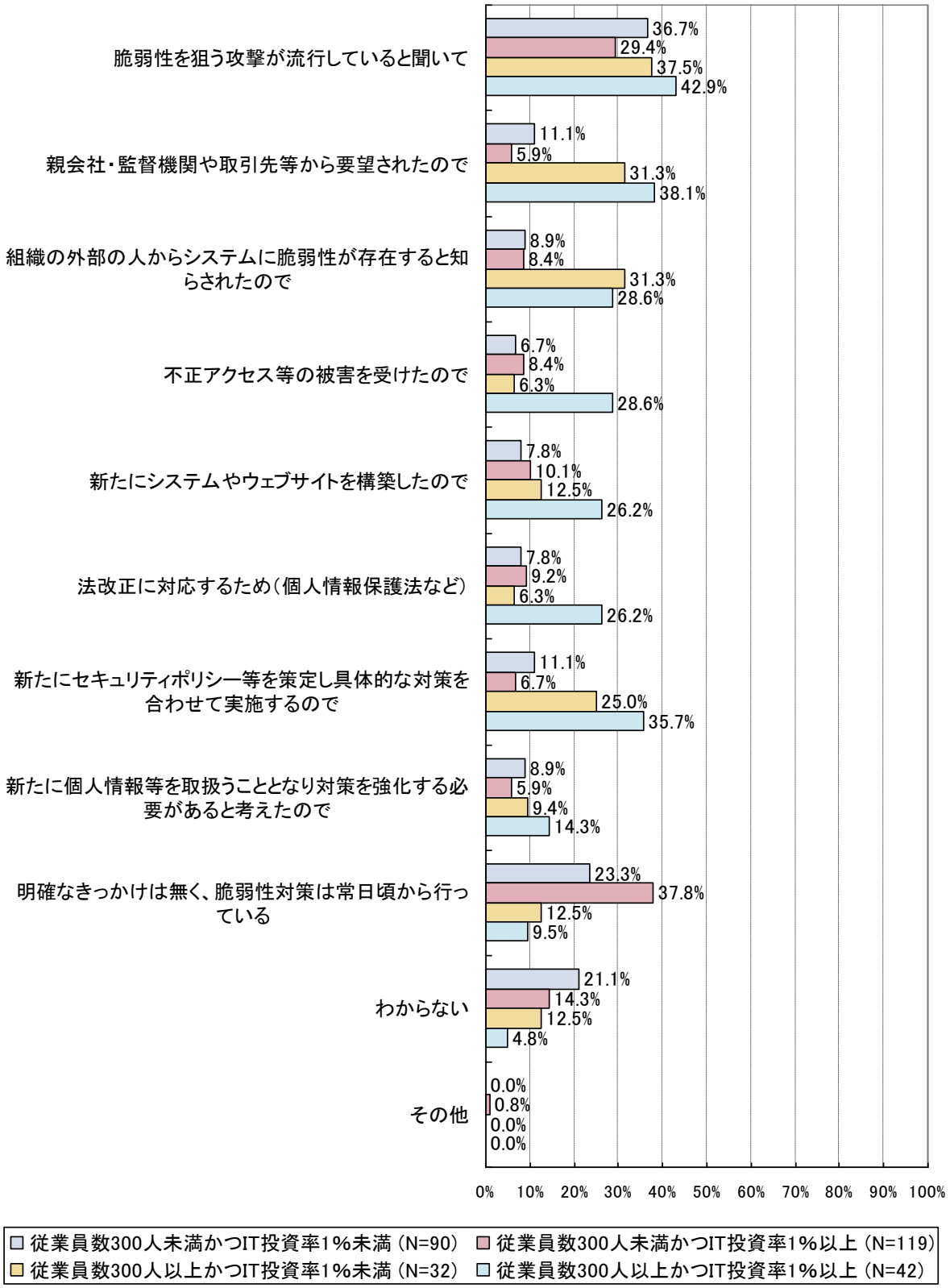

図 4.2-2　脆弱性対策をはじめたきっかけ（規模と IT 投資率別）

課題認識に関する設問では次のような傾向が見られた。「全サーバ等に脆弱性対策を行うの

は難しい」を課題に挙げる組織は大企業等において多い。これは企業の規模に合わせてシステムが大きくなり対策の徹底が難しくなるためと考えられる。

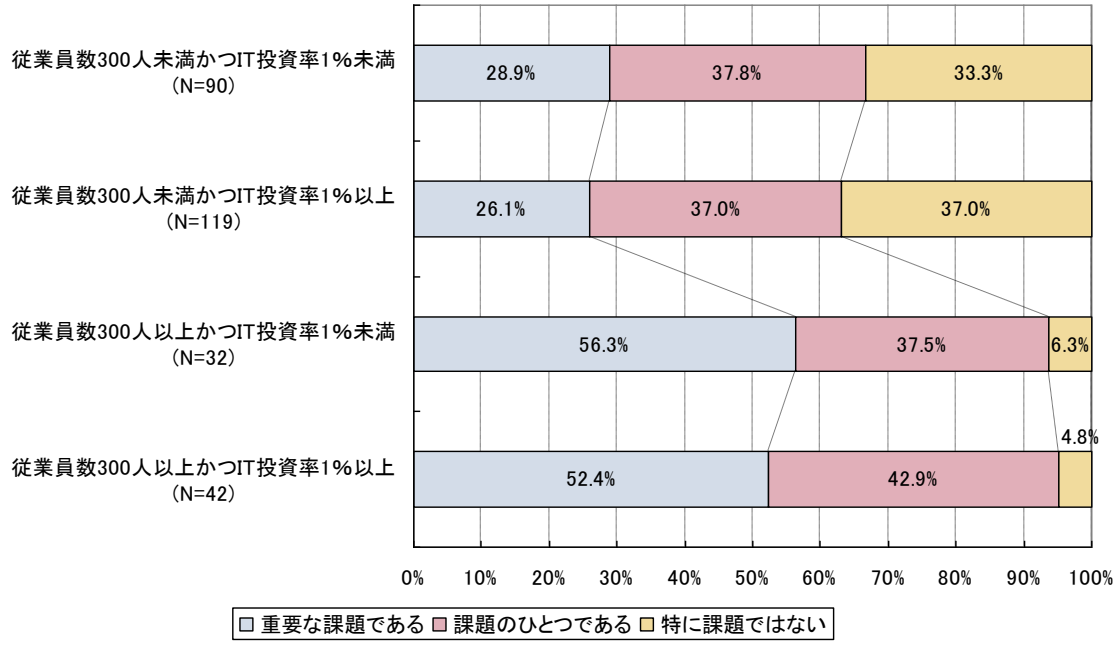

図 4.2-3　課題認識 ― 全サーバ等に脆弱性対策を行うのは難しい（規模と IT 投資率別）

大企業等で IT 投資率が高いグループにおいては「増え続ける脆弱性に逐一対応するのは難しい」ことが重要な課題とみなす傾向が顕著であった。IT 依存度が高い企業において対策を徹底しようとすると脆弱性に定常的な対処への難しさが課題となる様子が伺える。

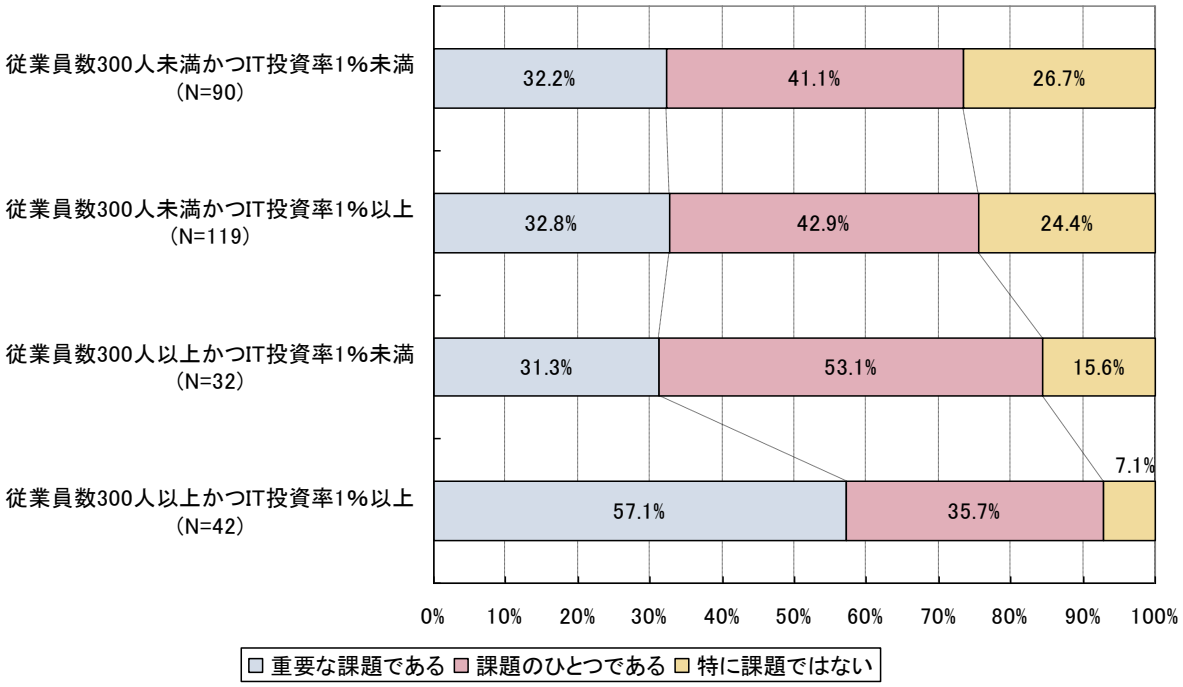

図 4.2-4　課題認識 ― 増え続ける脆弱性に逐一対応するのは難しい（規模と IT 投資率別）

他の課題に比べると「脆弱性に関する情報がどこにあるかわからない」を課題に挙げる組織は少なかった。情報収集の困難さは、解決が容易な課題といえるだろう。

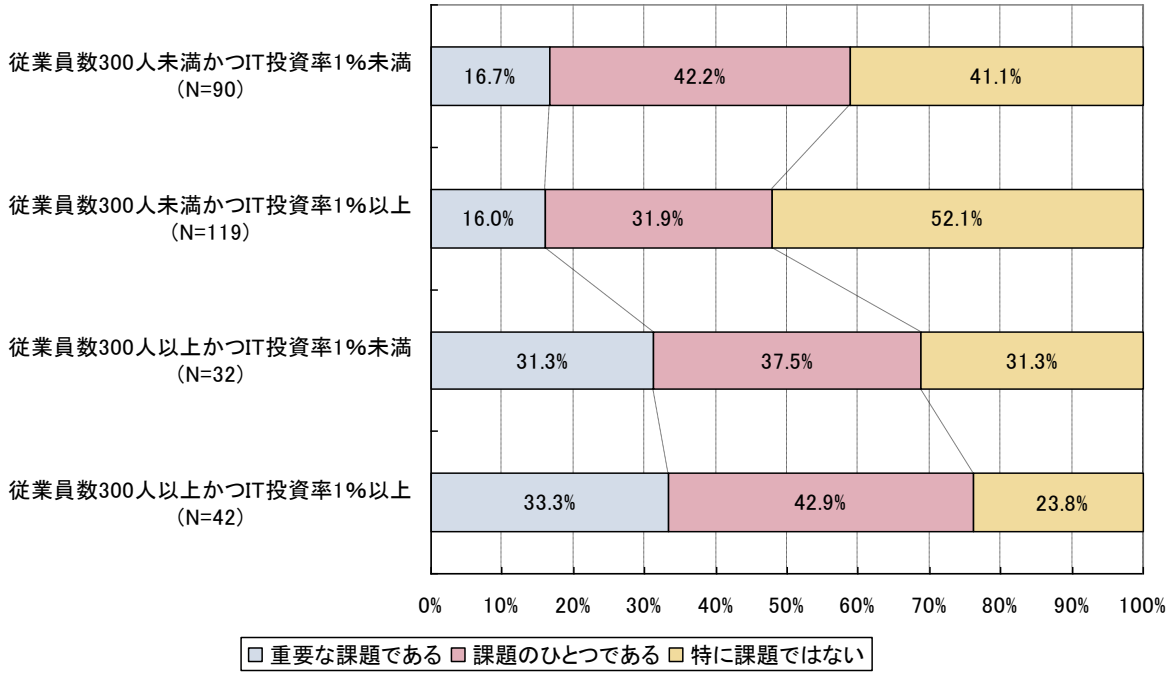

図 4.2-5　課題認識 ― 脆弱性に関する情報がどこにあるかわからない（規模と IT 投資率別）

「脆弱性対策にコストを要する（テストや実機への適用等）」を課題にあげる組織は多く、特に大企業等で IT 投資率が低いグループでは重要な課題とみなすとの回答が 50.0%にもなった。このグループは「社内外に脆弱性対策の体制・人員が整っていない」という課題も重視しており、特に大企業で IT 依存度がそれほど高くない組織において、脆弱性対策のコストが問題となる傾向が見て取れる。

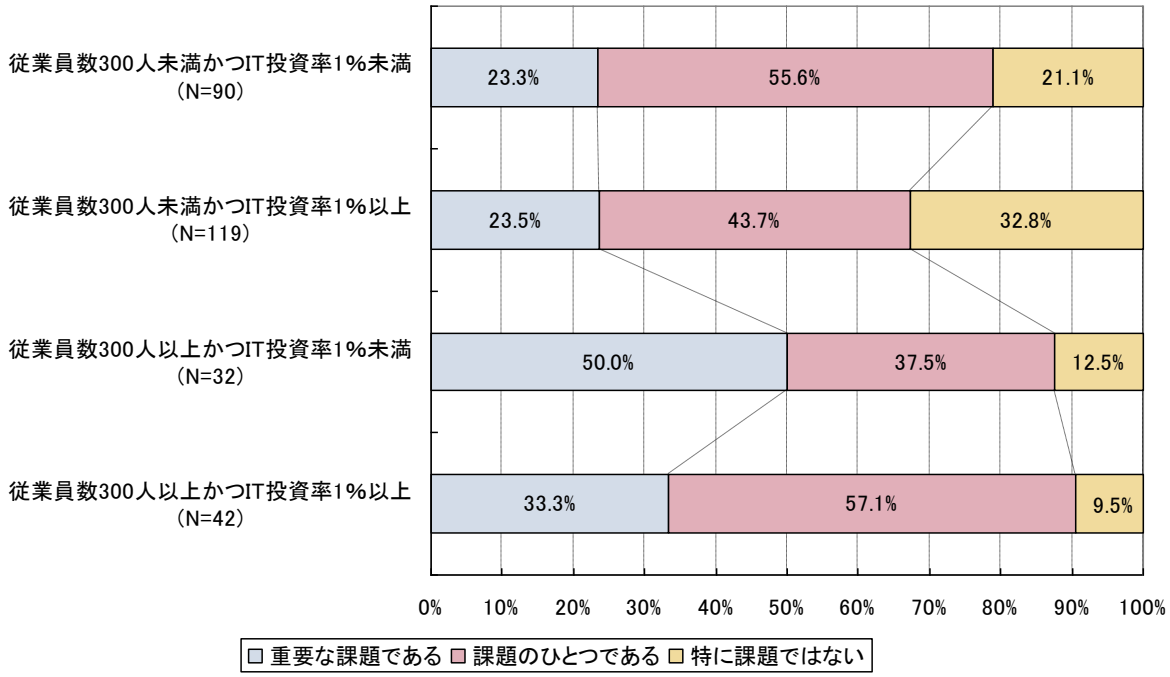

図 4.2-6　課題認識 ― 脆弱性対策にコストを要する（規模と IT 投資率別）

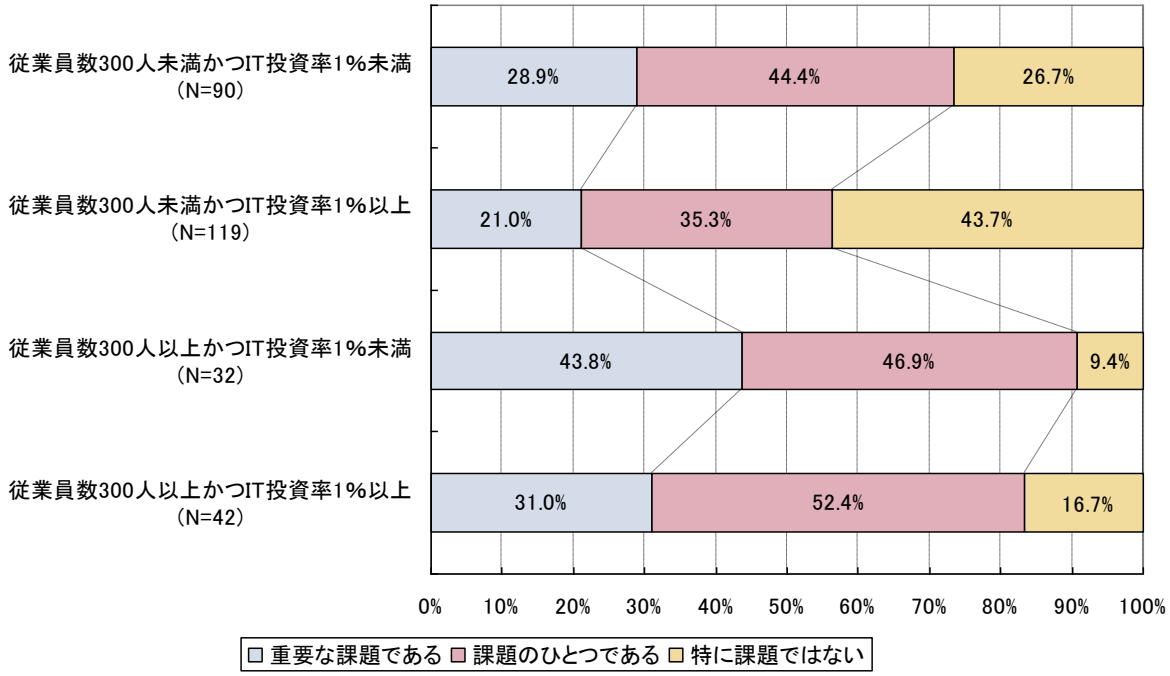

図 4.2-7　課題認識 ― 社内外に脆弱性対策の体制・人員が整っていない（規模と IT 投資率別）

「経営層の理解が乏しい」、「システムオーナー部門の理解が乏しい」、「組織内のユーザーの理解が乏しい」という課題については、中小企業等でＩＴ投資率が高いグループでは特に課題とみなす比率が少なかった。これは中小企業等であるが故に組織内の情報伝達が密で齟齬

が少ない点、加えて IT 投資が十分であることからセキュリティに関する予算・人員等も比較的確保されている点が、このグループにおいては組織内の理解不足は課題視するまでもなく解決されているためだろうと考えられる。

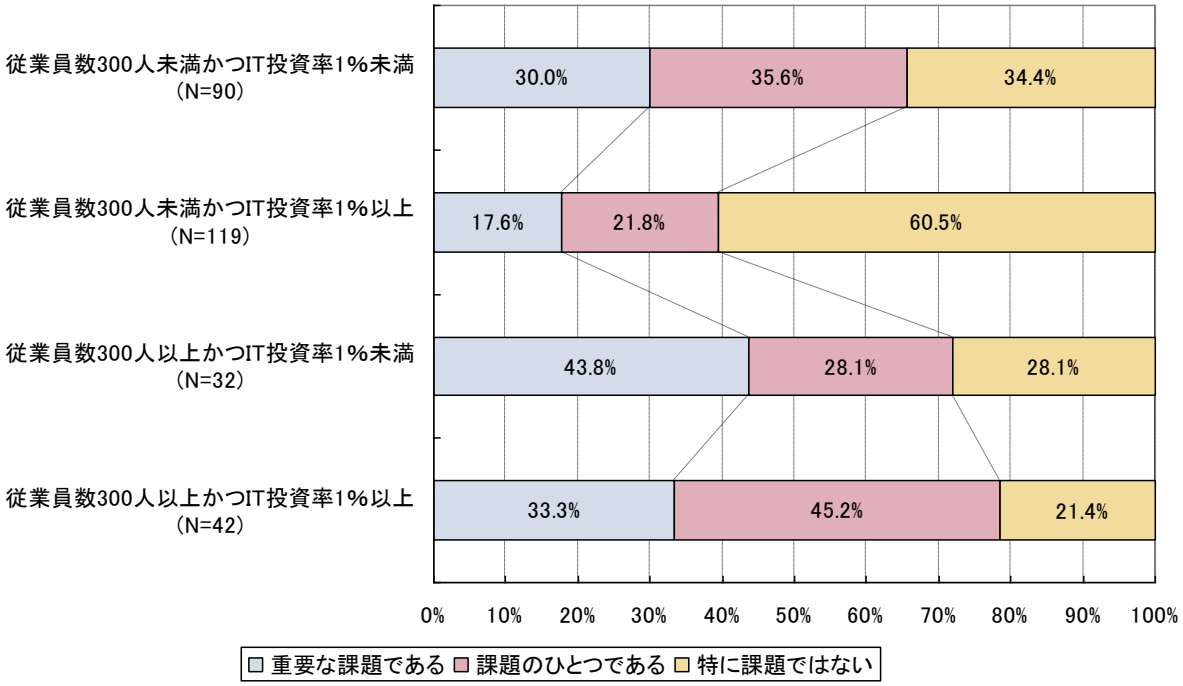

図 4.2-8　課題認識 ― 脆弱性対策について経営層の理解が乏しい（規模と IT 投資率別）

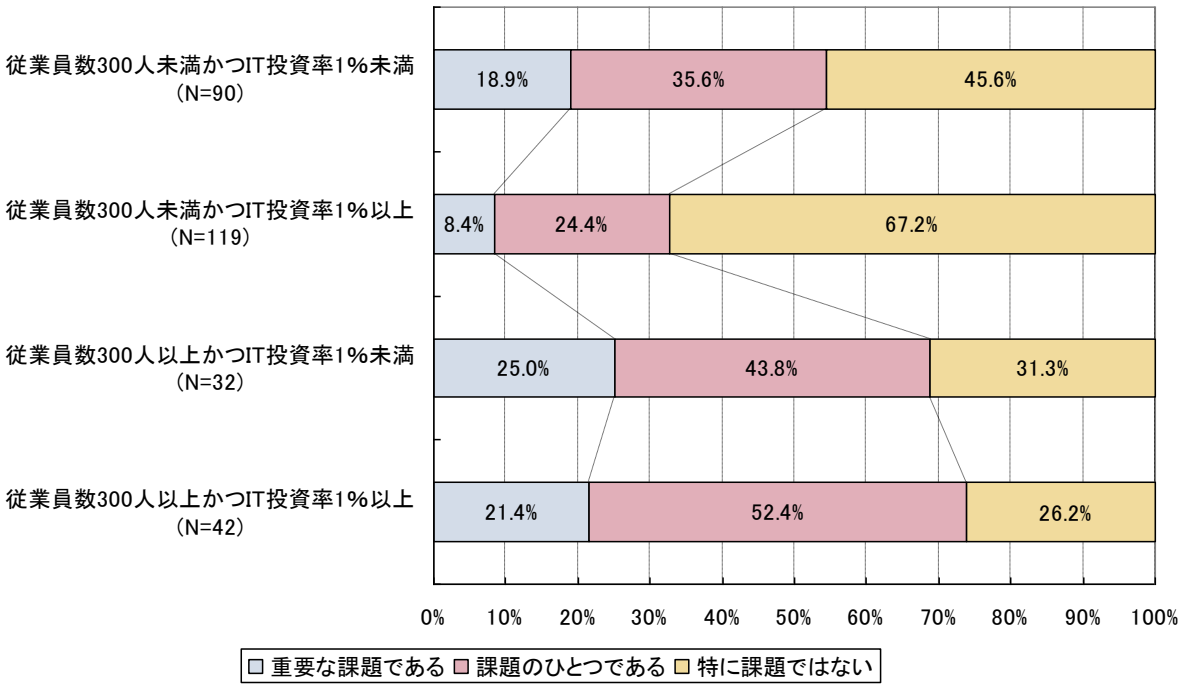

図 4.2-9　課題認識 ― 脆弱性対策についてシステムのオーナー部門の理解が乏しい（規模と IT 投資率別）

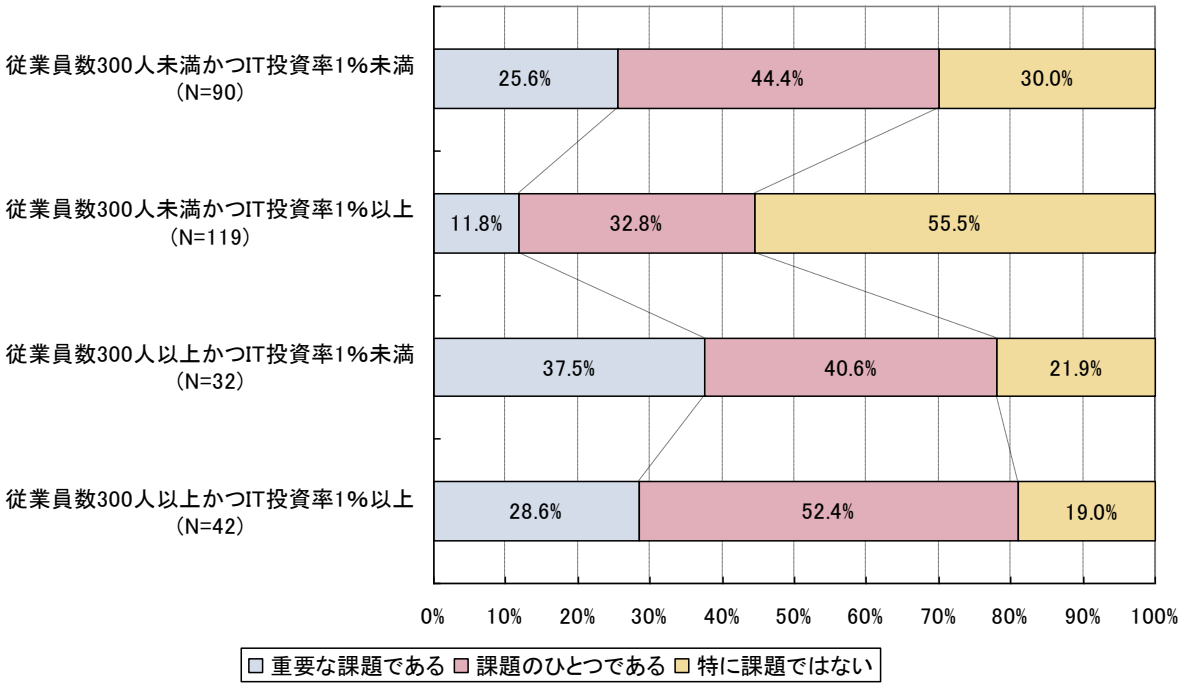

図 4.2-10　対策の課題認識 ― 脆弱性対策について組織内のユーザーの理解が乏しい（規模とIT 投資率別）

4.3.脆弱性対策の普及推進における課題

・ 運用中のシステムの脆弱性対策を外部委託する場合、「契約には明記されていないが、事実上、委託費用に全て含まれている」との解釈を示す回答が高い割合で見られた。増加する脆弱性の状況を考慮すれば、委託先の負担はバランスを欠いたものになりかねない。今後、改善に向けた取り組みがなされることを期待する。

・ ウェブサイトの脆弱性に気付くきっかけは、大企業等の 41.4%が「セキュリティ関連組織等から連絡を受けた」ことを挙げていること、また、大企業等の 33.3%、中小企業等の 18.2%が脆弱性対策の判断時に「セキュリティ関連組織等が提供する情報」を参考にしていることから、情報セキュリティ早期警戒パートナーシップの取り組みが効果を挙げていることがわかる。ただし、情報セキュリティ早期警戒パートナーシップや脆弱性関連情報届出受付（IPA)、製品開発者調整（JPCERT/CC)、JVN 等の認知度や利用経験にはまだ向上の余地がある。特に、中小企業等への啓発が遅れている状況の改善が望まれる。