

小規模ウェブサイト運営者の脆弱性対策に関する 調査報告書

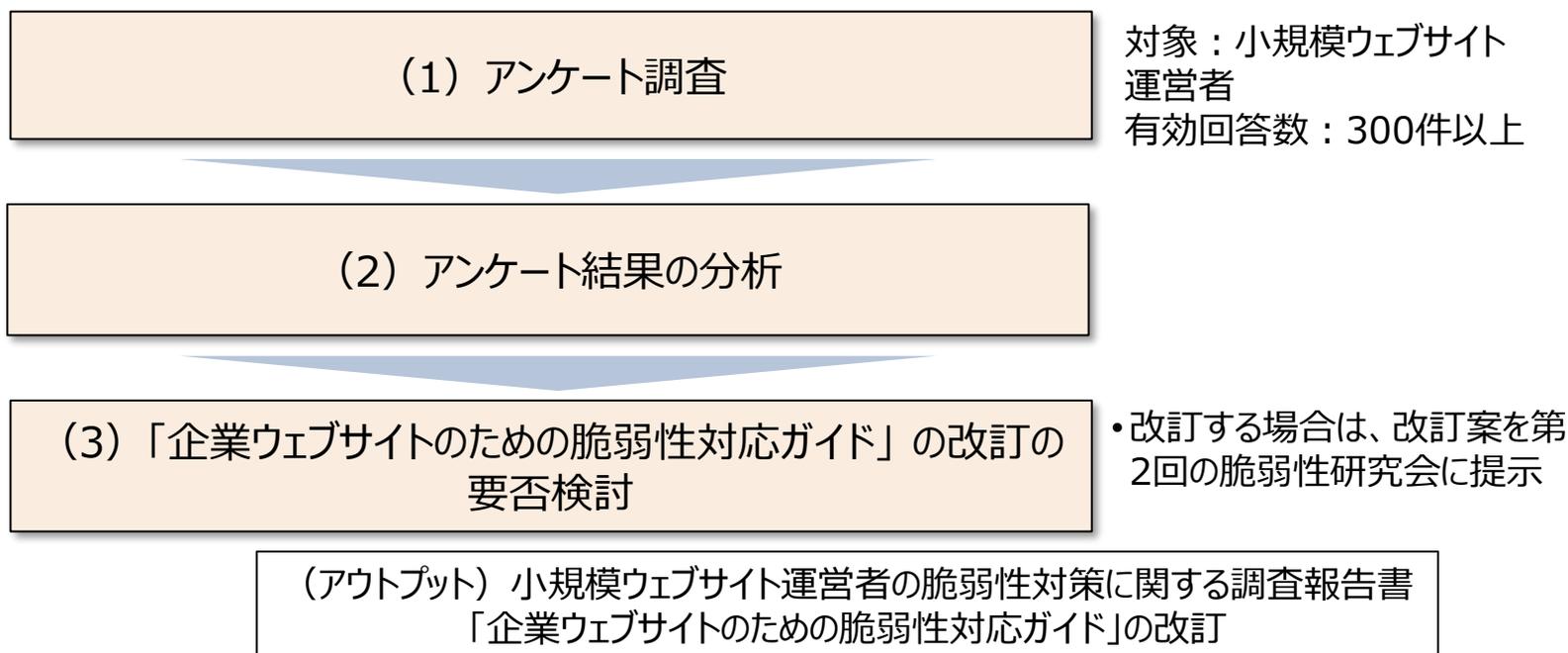
概要

2021年3月

独立行政法人 情報処理推進機構

1. 調査背景・検討概要

- ウェブサイトの脆弱性対処について、ウェブサイト運営者としての責務（望ましい対処）であることが認識されるよう普及啓発を実施してきている。しかし、パートナーシップでのウェブサイトに関する届出や修正対応の状況を踏まえると、特に小規模ウェブサイト運営者において脆弱性対策を進めるうえで課題があると推測される。
- このため、小規模ウェブサイト運営者における脆弱性対処の現状に関するアンケート調査を行い、その結果から導き出されるウェブサイト運営者としての課題を抽出するとともに、課題への対処方法をこれまでの脆弱性研究会での調査結果も踏まえて検討する。
- 調査結果及び検討結果は、「小規模ウェブサイト運営者の脆弱性対策に関する調査報告書」として取り纏めると共に、「ウェブサイトの最近の被害事例に関する調査」の調査結果と合わせて「企業ウェブサイトのための脆弱性対応ガイド」の改訂の可否を検討し、必要な改訂を行う。



IPA

2.アンケート調査

- 2012年度に実施した、小規模ウェブサイト運営者の脆弱性対策に関するアンケート調査と同様な調査を再度実施をして、現時点における小規模ウェブサイト運営者の脆弱性対策の状況を調査した。
アンケート調査にあたっては、以下を実施した。

[成果物]

小規模ウェブサイト運営者の脆弱性対策に関する調査報告書

[調査対象と件数]

対象：2012年度のアンケート調査と同様に小規模ウェブサイト※を運営する組織のウェブサイト担当や情報システム担当
(経年変化を調査するため、可能な限り2012年度のアンケート対象を取り込む。)

有効回答数：301件

※中小企業基本法において定義された「小規模企業者」(おおむね常時使用する従業員が20人以下、商業・サービス業で従業員5人以下の事業者)を含むよう、従業員が50名以下の企業を対象とした。

[調査方法]

ウェブアンケート調査

[調査項目]

以下の調査項目を全体で30項目程度(選択式、「その他」の記述は必要)

1. ウェブサイトの構築・運用の形態や内容
2. 脆弱性対策への理解
3. 脆弱性対策の現状と課題
4. IPAの普及啓発資料に関する認知度(活用度)

IPA 3.2012年度調査からの継続設問と仮説の検証

- 下記の仮説は、2012年度の仮説検証の結果に基づくものである。仮説1、2、6、9は半数程度の組織に妥当することが確認された（○）。仮説4については、「主に大企業が狙われており小企業は攻撃されないという考え」（著名ではなく攻撃されない）は前回から回答が減少しており、危機感のないことの主だった理由とはいえなかった（△）。

大項目	No.	結果	仮説内容	対応	問No.
ウェブサイトの構築・運用の実態	仮説1	○	自社社員が少人数（ほぼ1名）で運用者が不明確	予備調査	9
				本調査	9 25
	仮説2	○	構築および運用の方針は経営者が決定	本調査	5 22
脆弱性対策への理解	仮説3	◎	セキュリティ対策は運用段階での対策を実施している	本調査	17 19
					仮説4
	仮説5	◎	脆弱性対策が脅威への根本的解決策となることを理解していない	本調査	11 20
脆弱性対策の現状と課題	仮説6	○	ウェブサイトを一時的に停止し修正作業が必要な脆弱性対策を行うことに消極的	本調査	26(6) 26(8) 26(9)
					仮説7
	仮説8	◎	セキュリティ技術が担当者には難しく理解し難い	本調査	8 26(2)
脆弱性対策の現状と課題	仮説9	○	トラブルが生じて脆弱性対策による根本的な解決は行われたい	本調査	19 23 24
IPAの普及啓発資料に関する認知度	仮説10	◎	無償で利用可能な良いコンテンツがあるならば利用したい	本調査	27 28

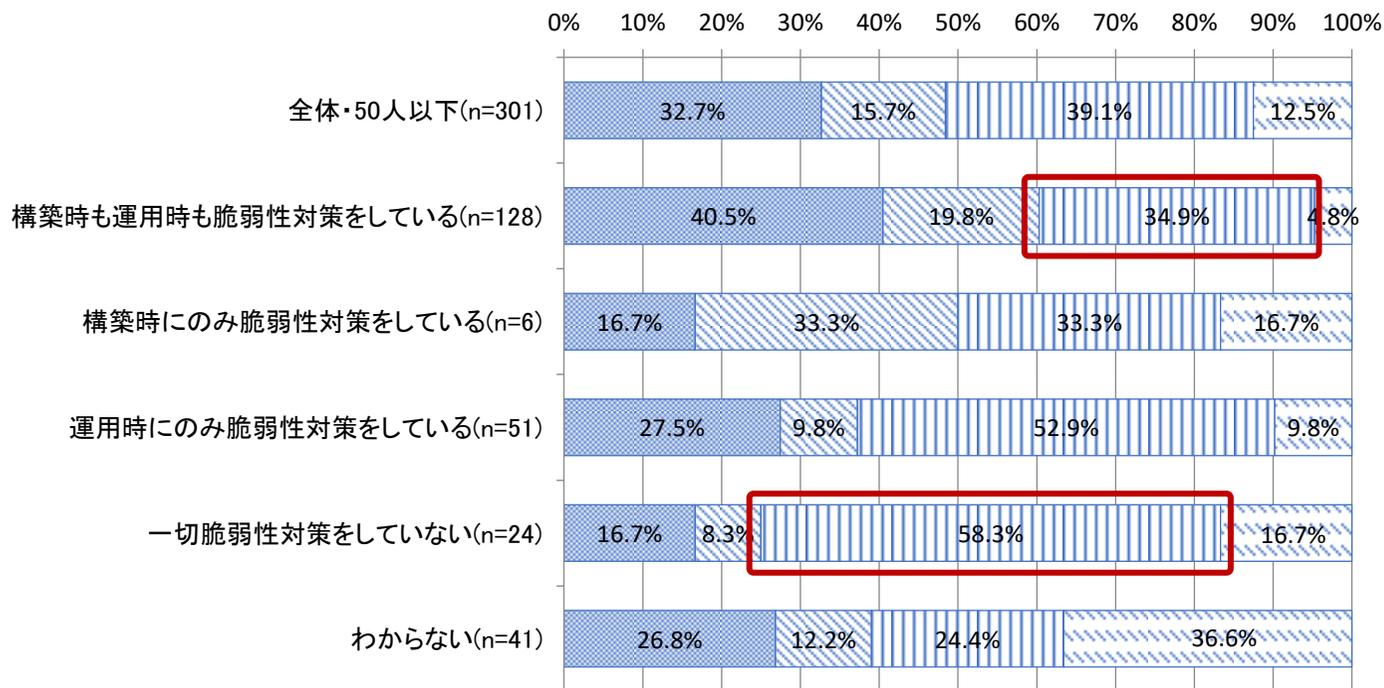
IPA 4.本年度調査の追加設問と仮説

- 下記の本年度で追加した仮設・設問を示す。
- 追加仮説1、3は半数程度の企業に妥当するものだった（○）。
- 追加仮説4は、複合的に対策を実施している企業が過半数を超える結果となった（△）。

No.	結果	仮説内容	対応	問No.	質問内容
追加 仮説 1	○	基本的なセキュリティ対策は、10年前と比較しても変化せず、実施している中小企業は少ない	本調査	13	貴社のウェブサイトでは 基本的な脆弱性対策 を、それぞれ実施していますか。
				7	貴社のウェブサイトは、 構築して何年経過 していますか。
追加 仮説 2	◎	ウェブサイトの役割や重要性が高まっているが、脆弱性対策やセキュリティ対策にかかるコストは変わらない	本調査	6	この10年くらいで、貴社における ウェブサイトの重要性や事業影響度等 がどの様に変化しましたか？
				14	この10年くらいで、貴社のウェブサイトの セキュリティ対策、脆弱性対策に掛かるコスト は、どの様になりましたか？
				16	この10年くらいで、貴社の ウェブサイト構築に掛かるコスト がどの様になりましたか？
				18	この10年くらいで、貴社の ウェブサイトの運用(管理や更新作業を含む)に掛かるコスト がどの様になりましたか？
追加 仮説 3	○	クラウド等のサービス利用時に、セキュリティ対策は、サービス提供事業者が対応しているので、自組織の対応が不要と思っている	本調査	4	[外部サービス利用と回答した方にお尋ねします] 開発・構築及び運用・管理で利用しているサービスのセキュリティ対策については、 自社の責任範囲とサービス提供者の責任範囲が明確 になっていますか。
追加 仮説 4	△	運用時の脆弱性対策として何らかの対応が実施されてはいるが、複数の対策による複合的な対応まではなされていない	本調査	15	貴社のウェブサイトのセキュリティ対策、 脆弱性対策 として、 運用時に実施 しているものを、それぞれの項目であてはまるものを選択してください。

5.対策状況による相違点について (脆弱性対策状況 - 組織的セキュリティ管理の状況)

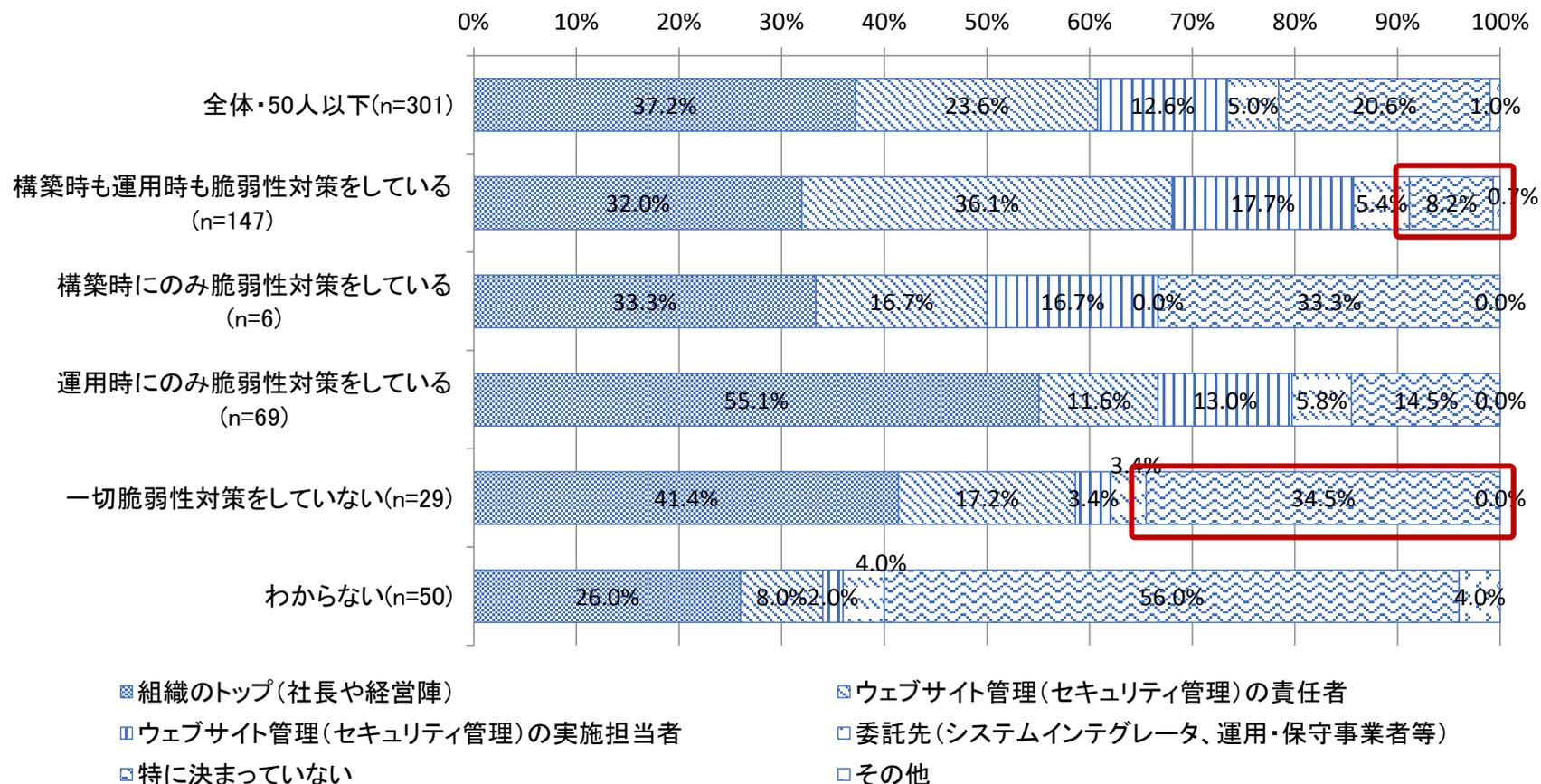
- 脆弱性対策の状況（問17、問19の集計結果）と組織のセキュリティ管理の状況（問9）についてクロス集計した結果を示す。
- 「構築時も運用時も脆弱性対策をしている」組織においては、セキュリティ管理を「組織的には行っていない（各自で対応している）」としたのは、34.9%であった。一方で「一切脆弱性対策をしていない」とした組織においてセキュリティ管理を「組織的には行っていない」組織は、58.3%にも及んだ。



- ウェブサイトのセキュリティの管理を行う担当者がいる(システム管理者など)
- 主担当の業務以外にウェブサイトのセキュリティの管理を兼任する担当者がいる(総務など)
- 組織的には行っていない(各自で対応している)
- わからない

IPA 5.対策状況による相違点について (脆弱性対策状況 - セキュリティ対策の判断を行う人)

- 脆弱性対策の状況（問17、問19の集計結果）とセキュリティ対策（脆弱性対策）の判断を行う人の状況（問22）についてクロス集計した結果を示す。
- 「構築時も運用時も脆弱性対策をしている」とした組織において判断を行う人が「特に決まっていない」としたのは、8.2%であった。一方で、「一切脆弱性対策をしていない」とした組織では、「特に決まっていない」が34.5%となった。



IPA 6.脆弱性対策が進んだ点、変化が少なかった点

- 本調査の結果として、2012年度調査と比較し、特に小規模ウェブサイト運営者の脆弱性対策が進んだ点、変化が少なかった点を報告する。

	脆弱性対策	組織体制
進んだ点	<ul style="list-style-type: none">・開発・構築する際に重視する点としてセキュリティが増加（問2）・構築時の脆弱性対策はしていないが減少（問17）	<ul style="list-style-type: none">・ウェブサイトのセキュリティ対策の管理を組織的に行っていないが減少（問9）・ウェブサイトのセキュリティ担当者が増加（問9）
変化の少なかった点	<ul style="list-style-type: none">・ウェブサイト運用時の脆弱性対策実施（問19）・ウェブサイトに脆弱性対策などのセキュリティ対策を進める上での課題（問26）・脆弱性対策・セキュリティ対策に関するIPAの各種資料の認知度（問28）	<ul style="list-style-type: none">・ウェブサイトの運用・構築に関する組織トップの関与（問5）・ウェブサイト運用・構築担当者の選定理由（問8）

IPA 7.まとめ

■小規模ウェブサイト運営者における脆弱性対策の現状に関するアンケート調査をもとに、課題への対処についての検討した結果を以下に報告する。

アンケート調査結果	企業ウェブサイトのための脆弱性対応ガイドへの対応
<ul style="list-style-type: none">・「脆弱性やセキュリティに関する技術の習得が難しい」を課題として認識している（重要な課題、課題のひとつのとの回答を合わせ）は約70%（問26）・同様に「脆弱性やセキュリティに関する情報がどこにあるかわからない」は約60%等と高い（問26）	<ul style="list-style-type: none">・小規模ウェブサイトの運営者に対して、脆弱性や脆弱性対策に必要な情報を集約し、基礎的な情報から技術習得が可能な情報を提供する必要がある。
<ul style="list-style-type: none">・脆弱性対策・セキュリティ対策に関するIPAの提供情報は約60%から80%が認知していない状況（問28）・ウェブサイトの脆弱性を悪用した攻撃によって組織が被害を受けている情報を「参考にしたい」が約70%と高い（問12）	<ul style="list-style-type: none">・ウェブサイトの脆弱性を悪用した攻撃による被害情報を提供する必要がある。
<ul style="list-style-type: none">・従業員5人以下の組織、従業員6人～30人以下の組織ともに「自社で運用・管理」、「ホスティング利用」が減少し、「クラウド利用」が増加。（問3）	<ul style="list-style-type: none">・クラウドサービスの利用や外部委託先に依頼する際に検討すべき点を提供する必要

アンケート調査結果概要（特徴的な結果）

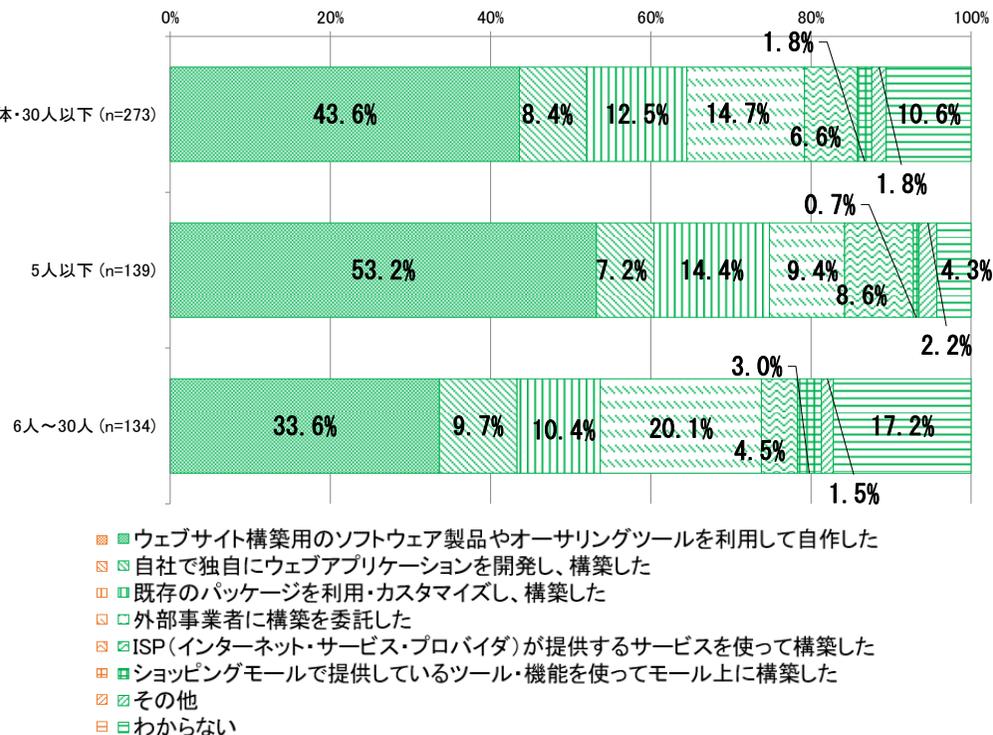
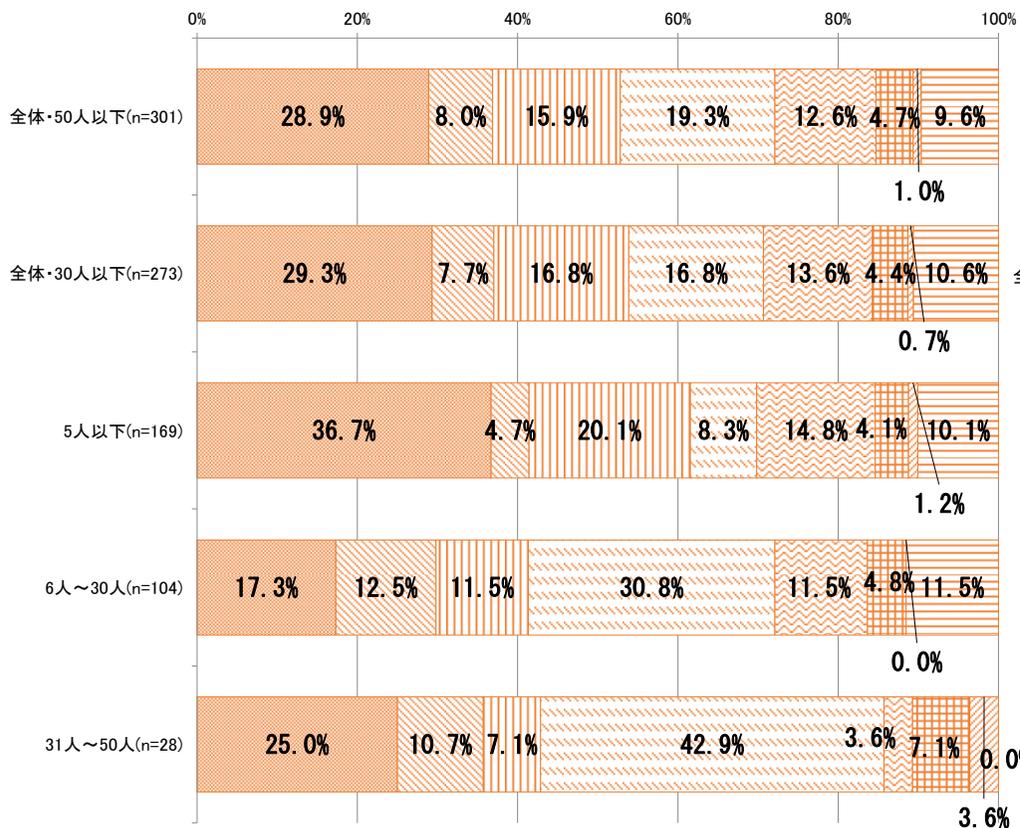
- | | |
|---------------------------------|--------------------------------|
| 問1：貴社で主要なウェブサイトを開発・構築した方法 | 問9：ウェブサイトのセキュリティ対策の管理・組織的な体制 |
| 問3：貴社のウェブサイトの運用・管理の形態 | 問11：ウェブサイトの脆弱性の認知度 |
| 問10：外部委託の際にセキュリティ対策に関するセキュリティ要件 | 問17：ウェブサイト構築時に実施している脆弱性対策 |
| 問2：貴社がウェブサイトを開発・構築する際、重視する点 | 問21：運用中のウェブサイト脆弱性対策が必要になったきっかけ |
| 問4：自社とサービス提供者の責任範囲 | 問22：ウェブサイトの脆弱性対策などの適用を判断する人 |
| 問6：この10年のウェブサイトの重要性や事業影響度の変化 | 問24：運用中のウェブサイトへの一時停止・該当箇所の作業担当 |
| 問16：この10年のウェブサイト構築に掛かるコストの変化 | 問27：「情報セキュリティ早期警戒パートナーシップ」の認知度 |
| 問18：この10年のウェブサイト運用に掛かるコストの変化 | 問28：脆弱性対策・セキュリティ対策に関する認知度 |
| 問7：ウェブサイトの構築何年と運用対策（クロス集計） | |

アンケート調査結果の表記（グラフ）について

2020年度調査では、従業員50人以下の総数301（うち、従業員数30人以下の総数273）に対して調査を実施した。2020年度調査を基に、2012年度調査結果（従業員数30人以下の総数273）と比較するために、2020年度調査結果のグラフは全体の集計値（従業員50人以下の総数301）に加え、2012年度調査結果と同じ従業員数30人以下に限定した集計値（従業員数30人以下の総数273）を併記している。
 なお、2020年度調査で新設した設問については2012年度調査との比較を行わないため、2020年度調査結果の全体の集計値（従業員50人以下の総数301）のみ掲載している。

問1：貴社で主要なウェブサイトを開発・構築した方法

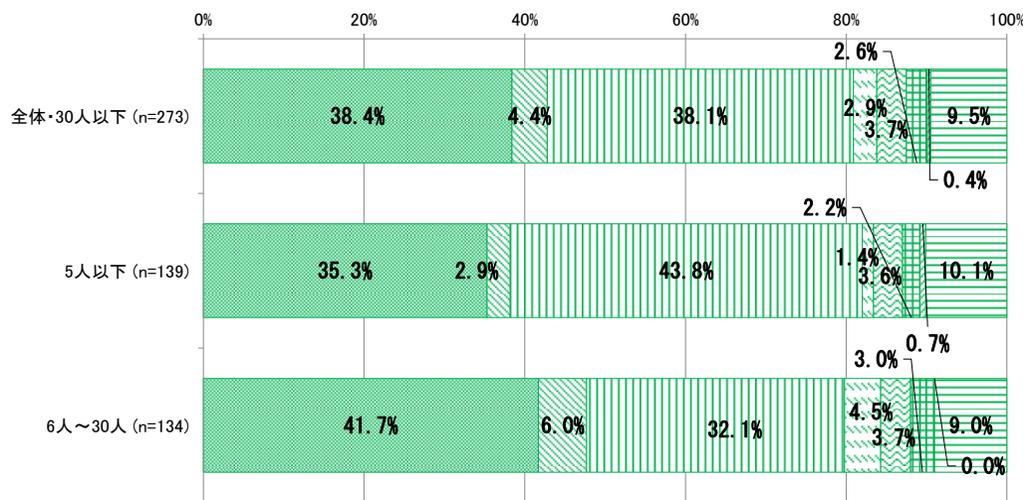
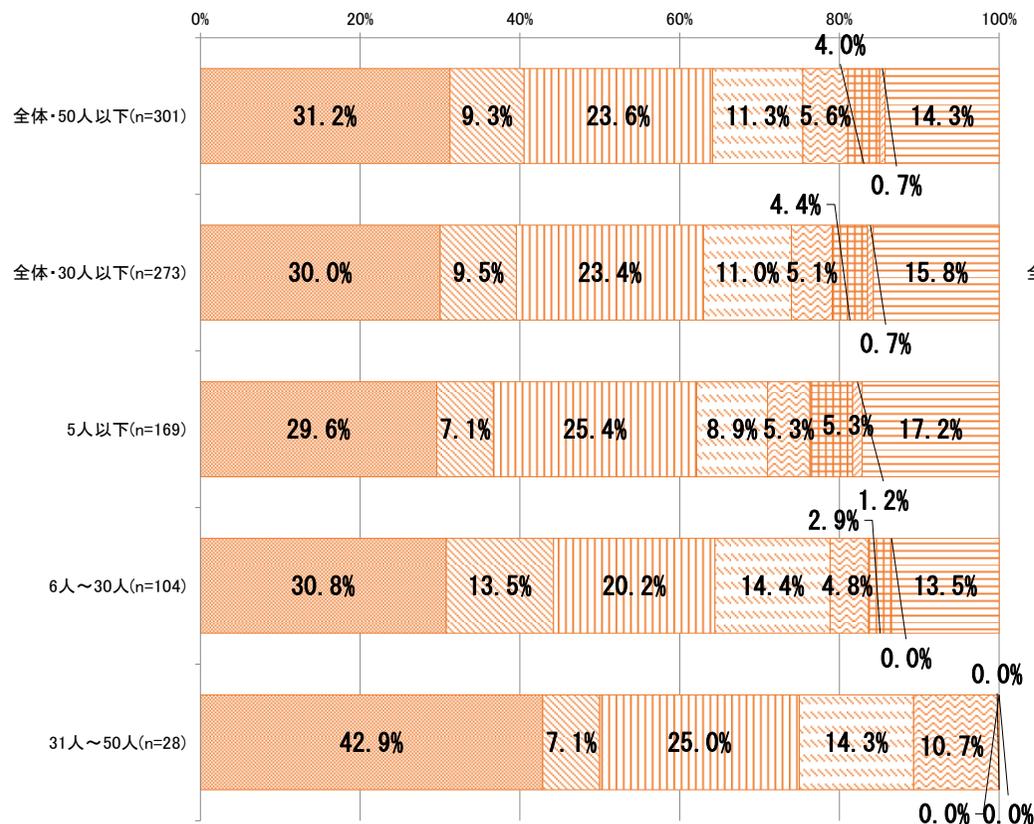
- 全体では、「自社開発（ウェブサイト構築用のソフトウェア製品やオーサリングツールを利用して自作）」が多い。
- 前回調査と比較し、「自社開発（ウェブサイト構築用のソフトウェア製品やオーサリングツールを利用して自作）」は本年度調査では29.3%であるが、前回調査では43.6%と高い。また、外部サービスを利用したウェブサイトの構築が多くなっている傾向がある。本年度調査では18.0%（ISP利用 13.6%、ショッピングモール利用 4.4%）であるが、2012年度調査では8.4%（ISP利用 6.6%、ショッピングモール利用 1.8%）であった。



- ウェブサイト構築用のソフトウェア製品やオーサリングツールを利用して自作した
- 自社で独自にウェブアプリケーションを開発し、構築した
- 既存のパッケージを利用・カスタマイズし、構築した
- 外部業者に構築を委託した
- ISP(インターネット・サービス・プロバイダ)が提供するサービスを使って構築した
- ショッピングモールで提供しているツール・機能を使ってモール上に構築した
- その他
- わからない

問3：貴社のウェブサイトの運用・管理の形態

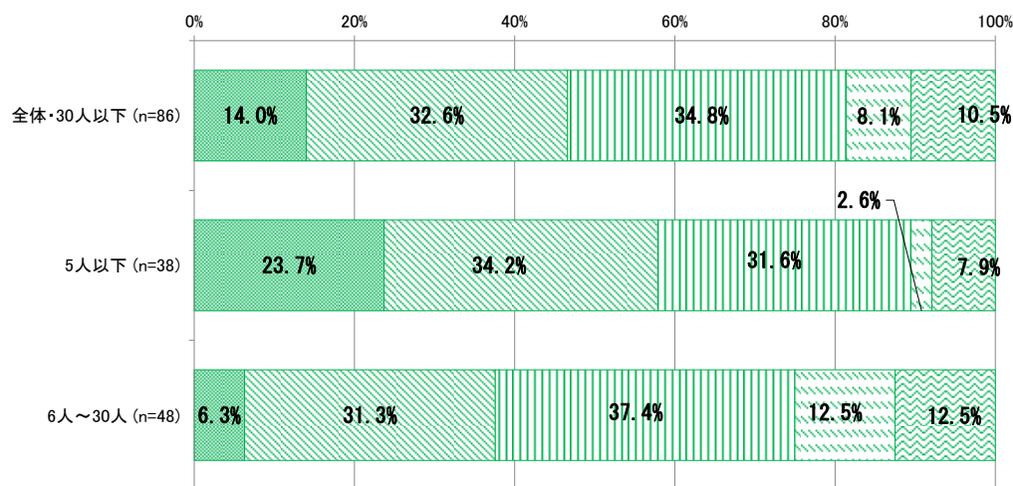
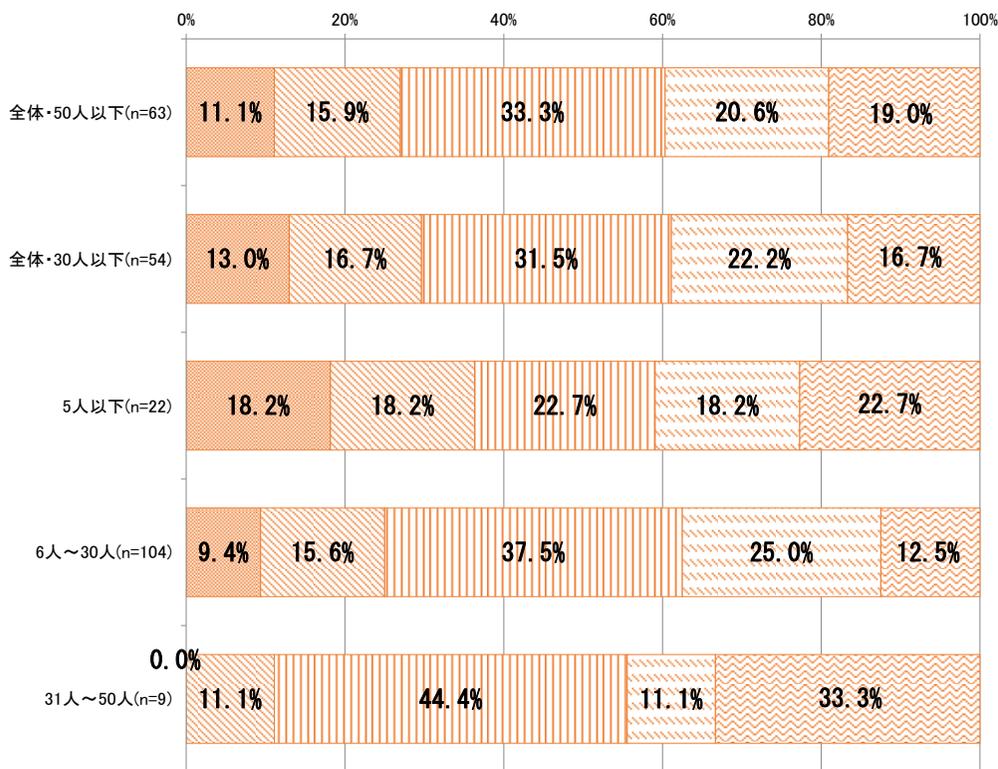
- 全体として、自社で運用・管理するという回答は合わせて40.5%であり、外部のサービスを利用しているという回答は合わせて44.5%であった。
- 前回調査と比較すると、ホスティングの利用が減り、クラウドの利用が増えている。



- 自社内で自社の社員がハードウェアからソフトウェアまですべて運用・管理している
- 自社内で委託先の社員がハードウェアからソフトウェアまですべて運用・管理している
- ホスティングを利用してウェブサイトを運用・管理している
- クラウド(IaaSやPaaS)上にウェブサイトを構築してウェブサイトを運用・管理している
- ASPサービスを利用してウェブサイトを運用・管理している
- ショッピングモール(楽天、Amazon等)を利用してウェブサイトを運用・管理している
- その他
- わからない

問10：外部委託の際にセキュリティ対策に関するセキュリティ要件

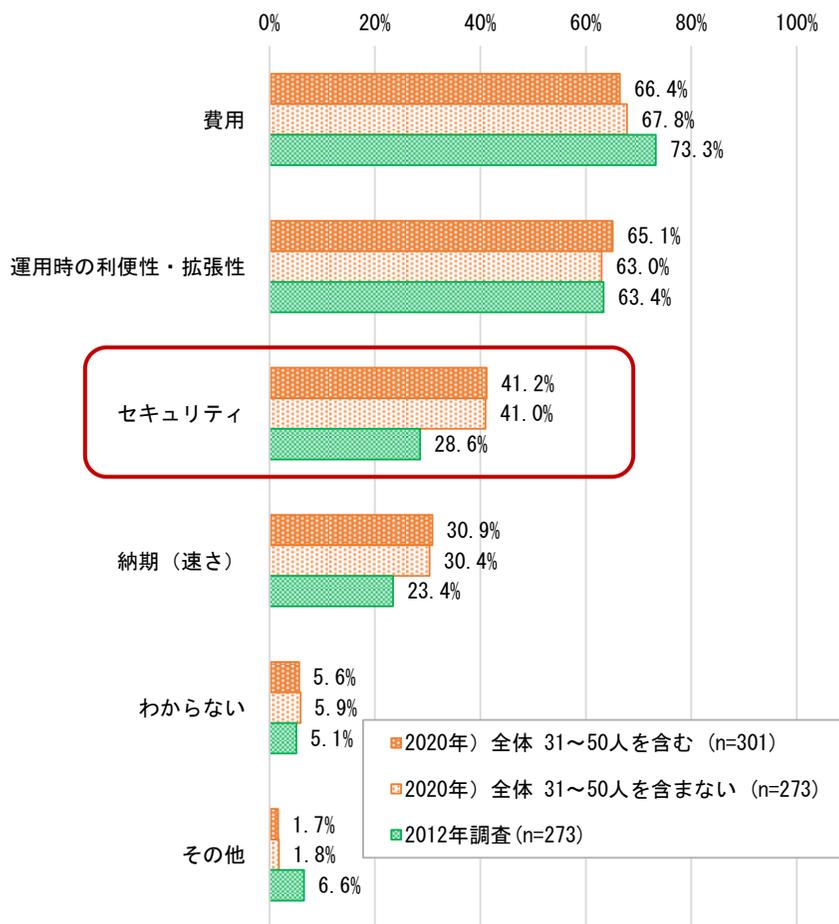
- 全体として、「セキュリティ要件は契約に含まれている」、「セキュリティ要件は契約に含まれており、委託先に積極的に要求する」というセキュリティ要件が契約に含まれているとの回答は合わせて53.9%であった。
- 本年度調査では、契約に必須ではないという回答が合わせて29.7%、前回調査では46.6%であった。また、「セキュリティ要件は契約に含まれており、委託先に積極的に要求する」が増加している傾向があり、本年度調査では22.2%、2012年度調査では8.1%であった。



- セキュリティ要件については特に気にしていない
- ▨ セキュリティ要件について気にはなるが、契約に必須ではない
- ▤ セキュリティ要件は契約に含まれている
- ▧ セキュリティ要件は契約に含まれており、委託先に積極的に要求する
- ▩ わからない

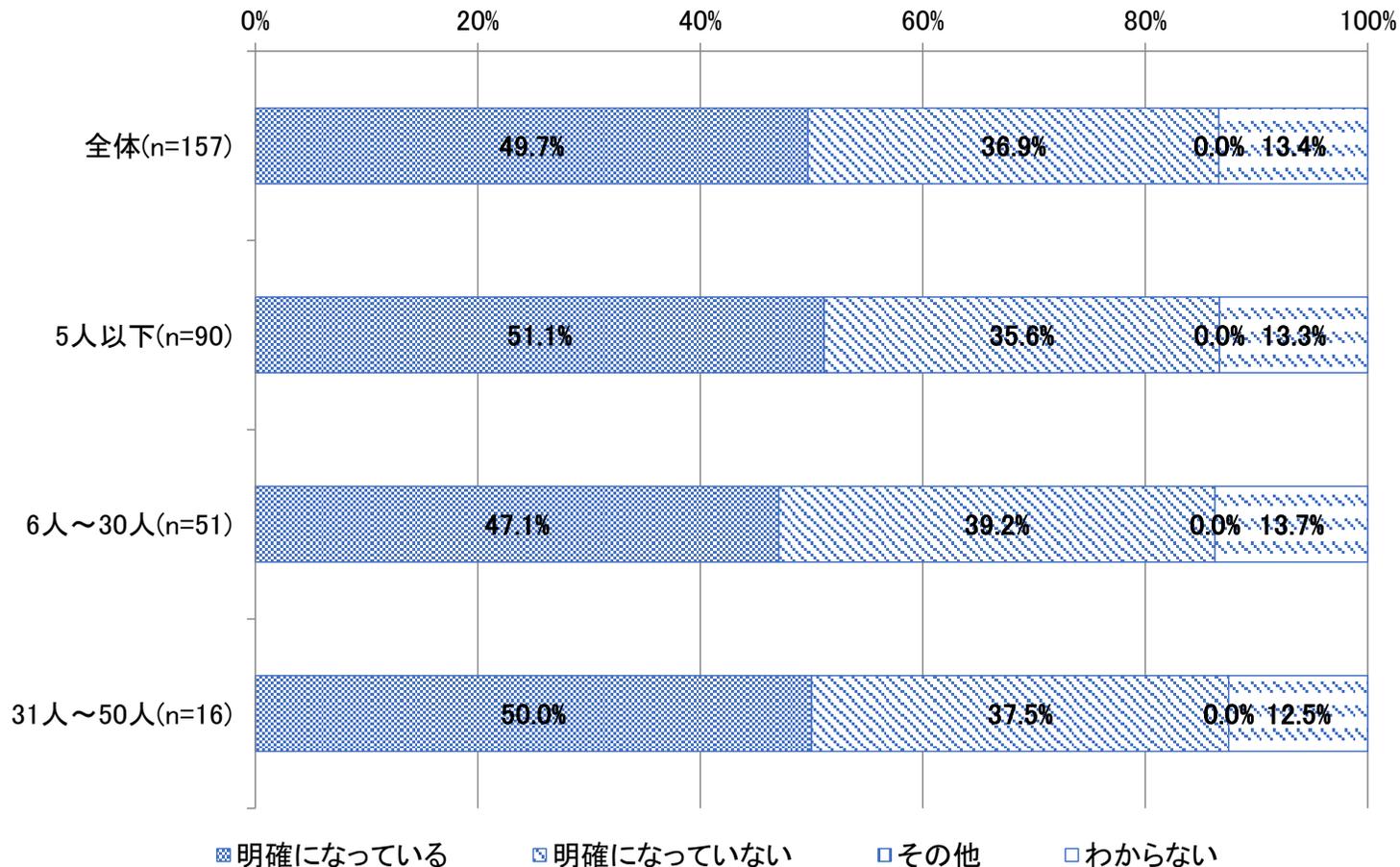
問2：貴社がウェブサイトを開発・構築する際、重視する点

- 全体としては、「費用」が66.4%、「運用時の利便性・拡張性」が65.1%であり、「費用」と「運用時の利便性・拡張性」が上位を占めた。この傾向は、2012年度調査においても同様である。
- 前回調査と比較し、セキュリティを重視する回答が増加した。



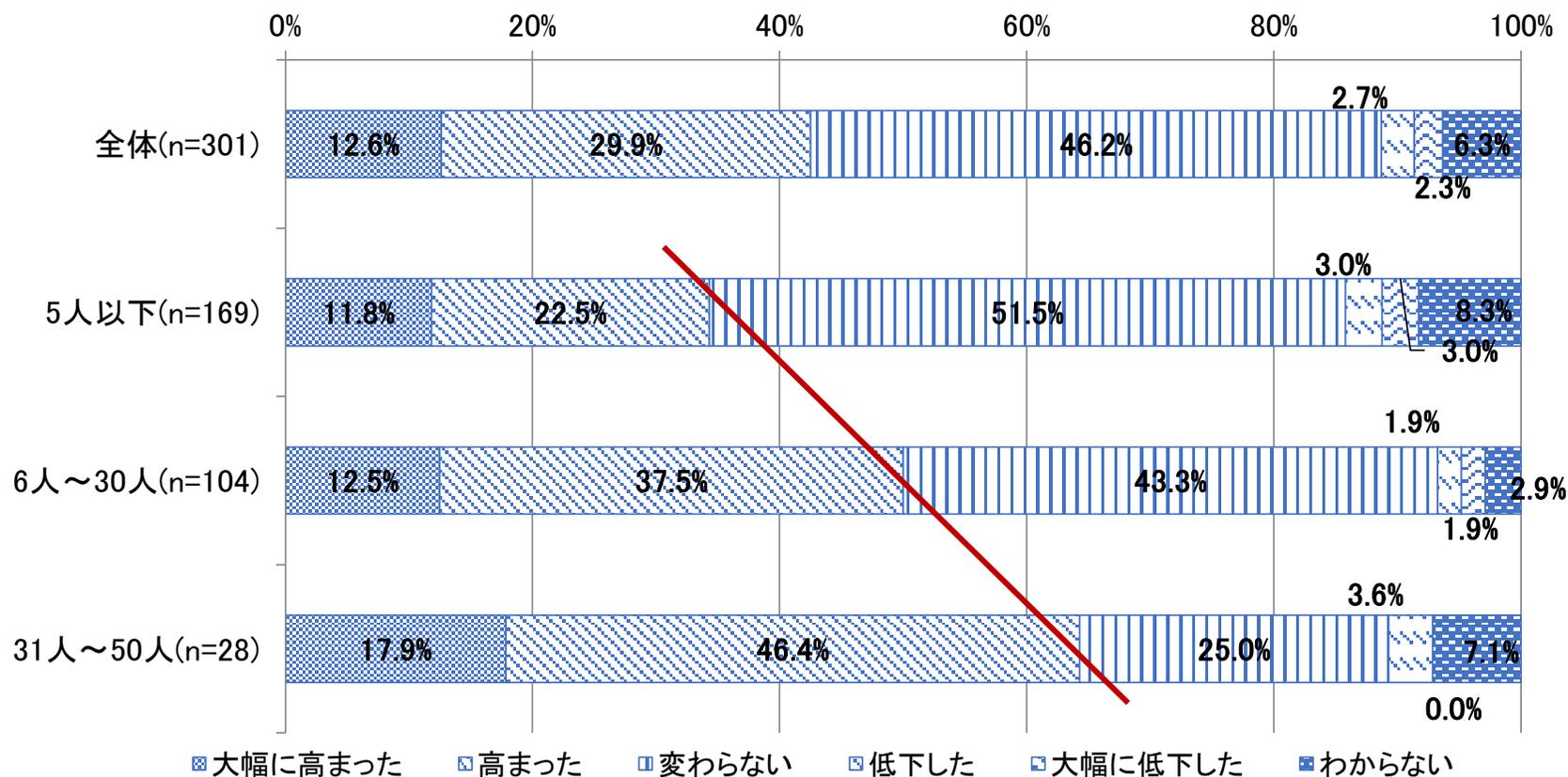
問4：セキュリティ対策に関する自社とサービス提供者の責任範囲(追加)

- 全体としては、「明確になっている」が49.7%と最も多く、次いで「明確になっていない」が36.9%であった。
- また、従業員数別でも同様の傾向であった。



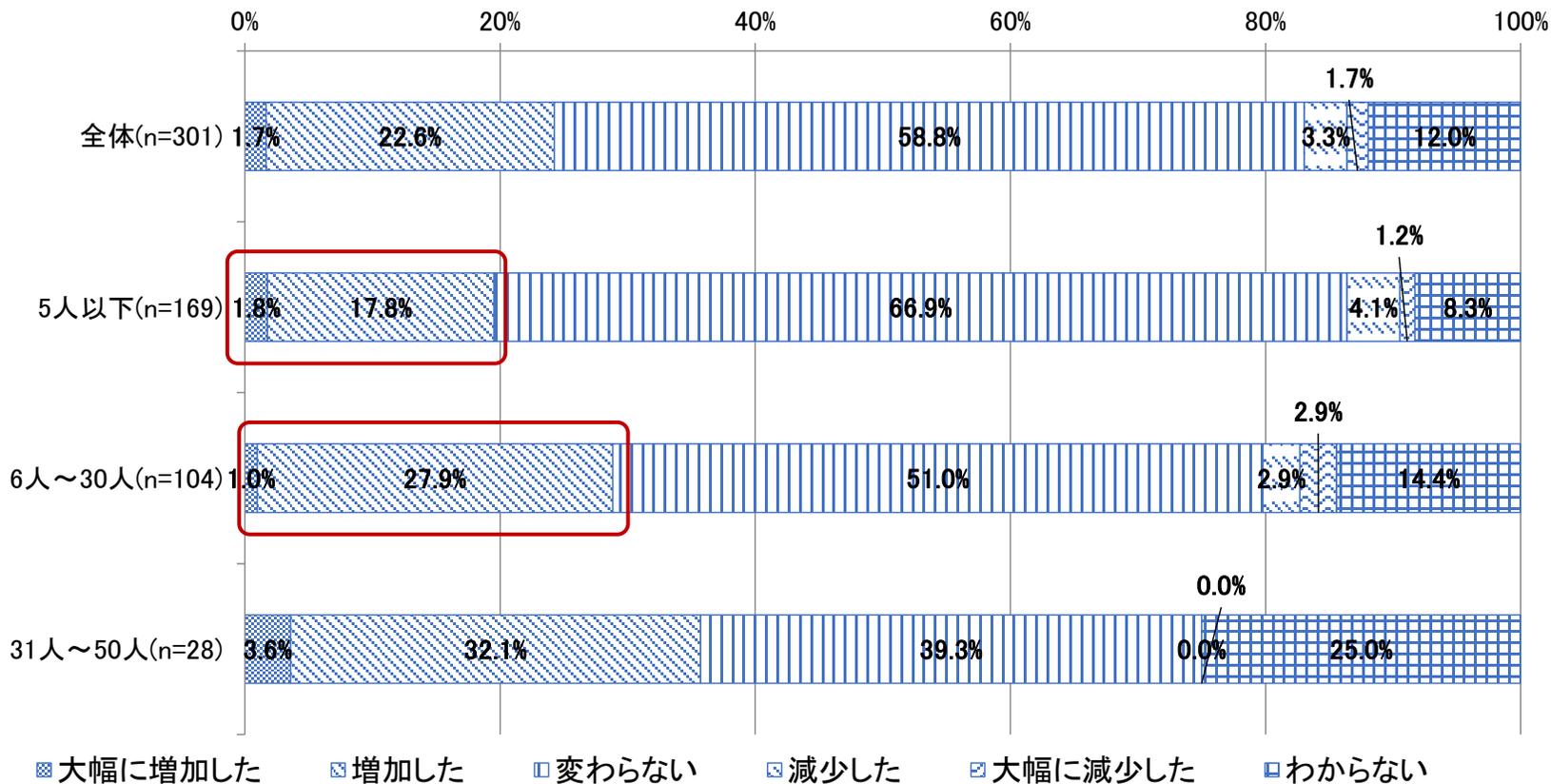
問6：この10年のウェブサイトの重要性や事業影響度の変化

- 全体では、「変わらない」という回答が46.2%と最も多く、次いで「大幅に高まった」、「高まった」という回答の合計は42.5%と多い傾向にある。
- 従業員数が多いほど重要性や事業影響度が高まったと感じている傾向がある。



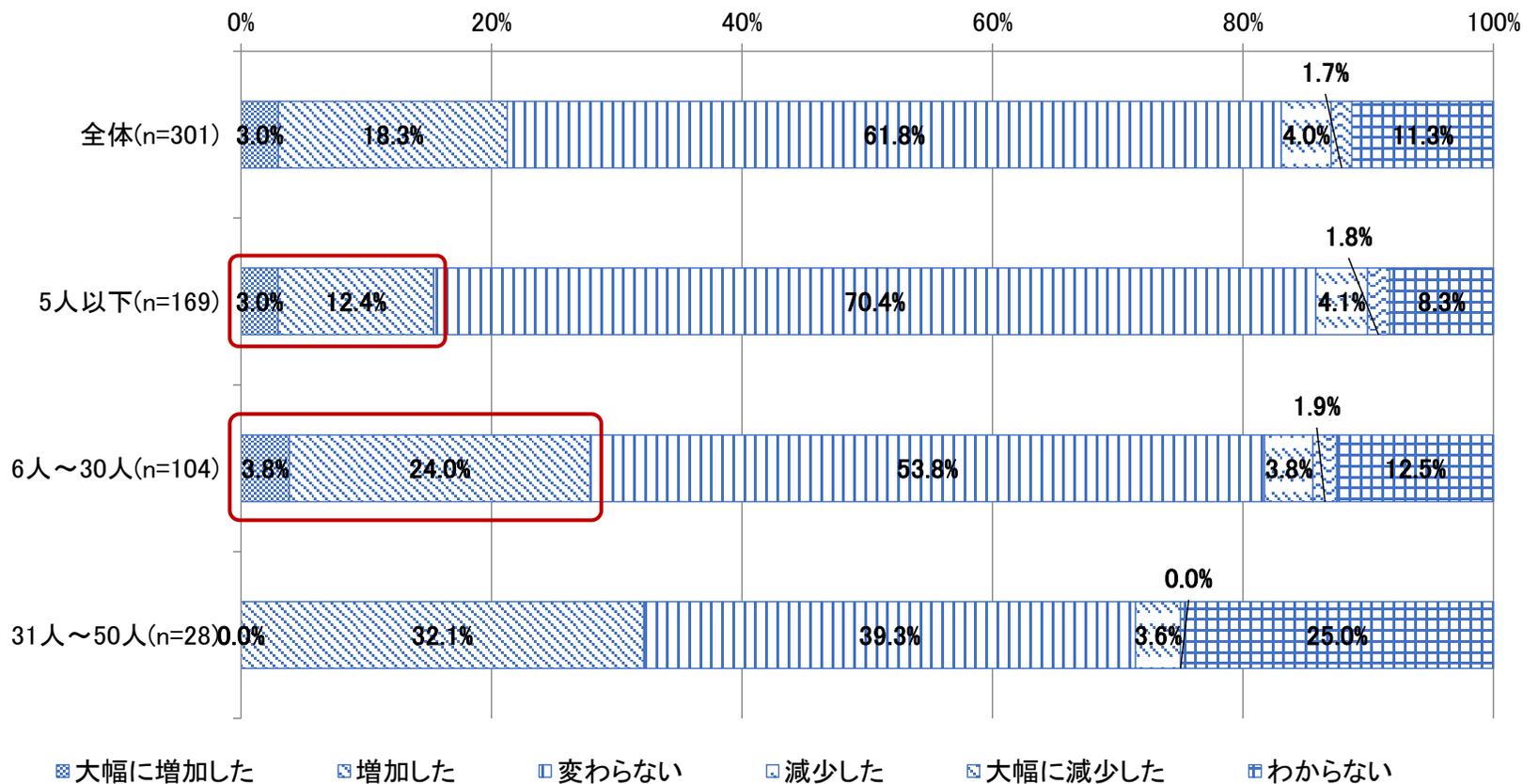
問16：この10年のウェブサイト構築に掛かるコストの変化

- 全体では、「変わらない」が58.8%と最も高く、次いで「大幅に増加した」、「増加した」の合計24.3%である。
- 従業員数が多いほどウェブサイトの構築コストが増加している傾向がある。



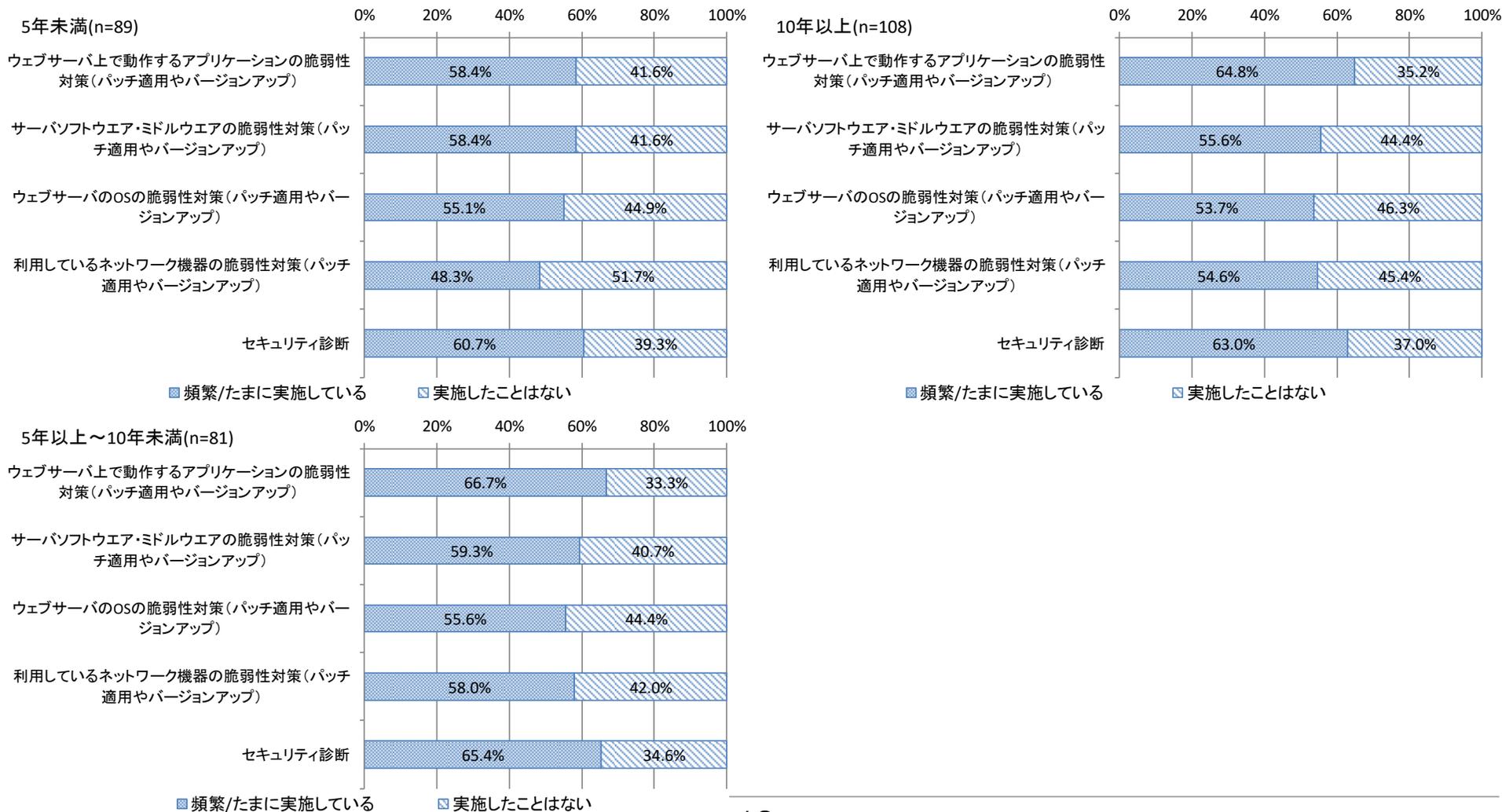
問18：この10年のウェブサイト運用に掛かるコストの変化

- 全体では、「変わらない」が61.8%と最も高く、次いで「大幅に増加した」、「増加した」の合計21.3%である。
- 従業員数が多いほどウェブサイトの運用コストが増加している傾向がある。



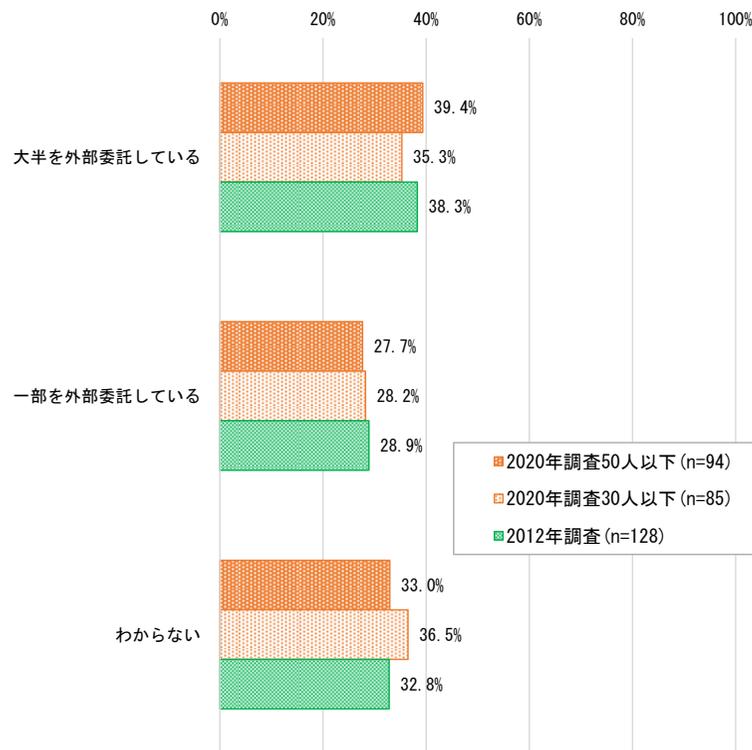
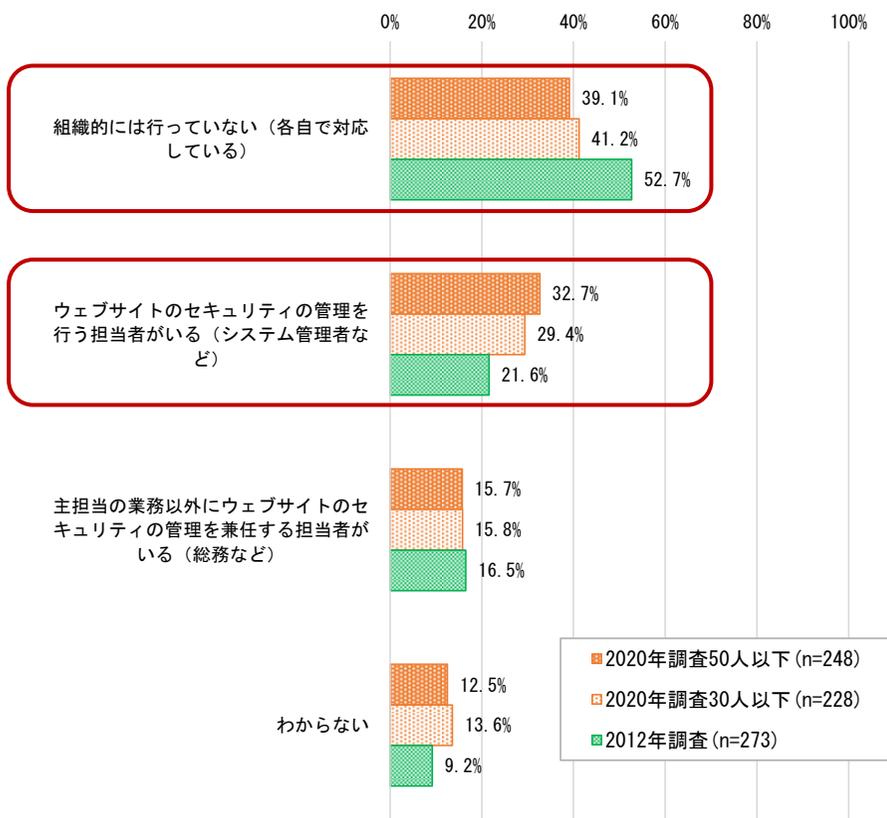
問7：ウェブサイトの構築年数と運用時の対策（問15とのクロス集計）

- ウェブサイトの構築年数ごとの運用時対策は、5年未満（左上）、5年以上～10年未満（左下）、10年以上（右上）で運用時の対策の大きな変化は見られないが、「5年以上～10年未満」と「10年以上」を比較すると、「10年以上」の方が各対策の実施率が低くなっている。



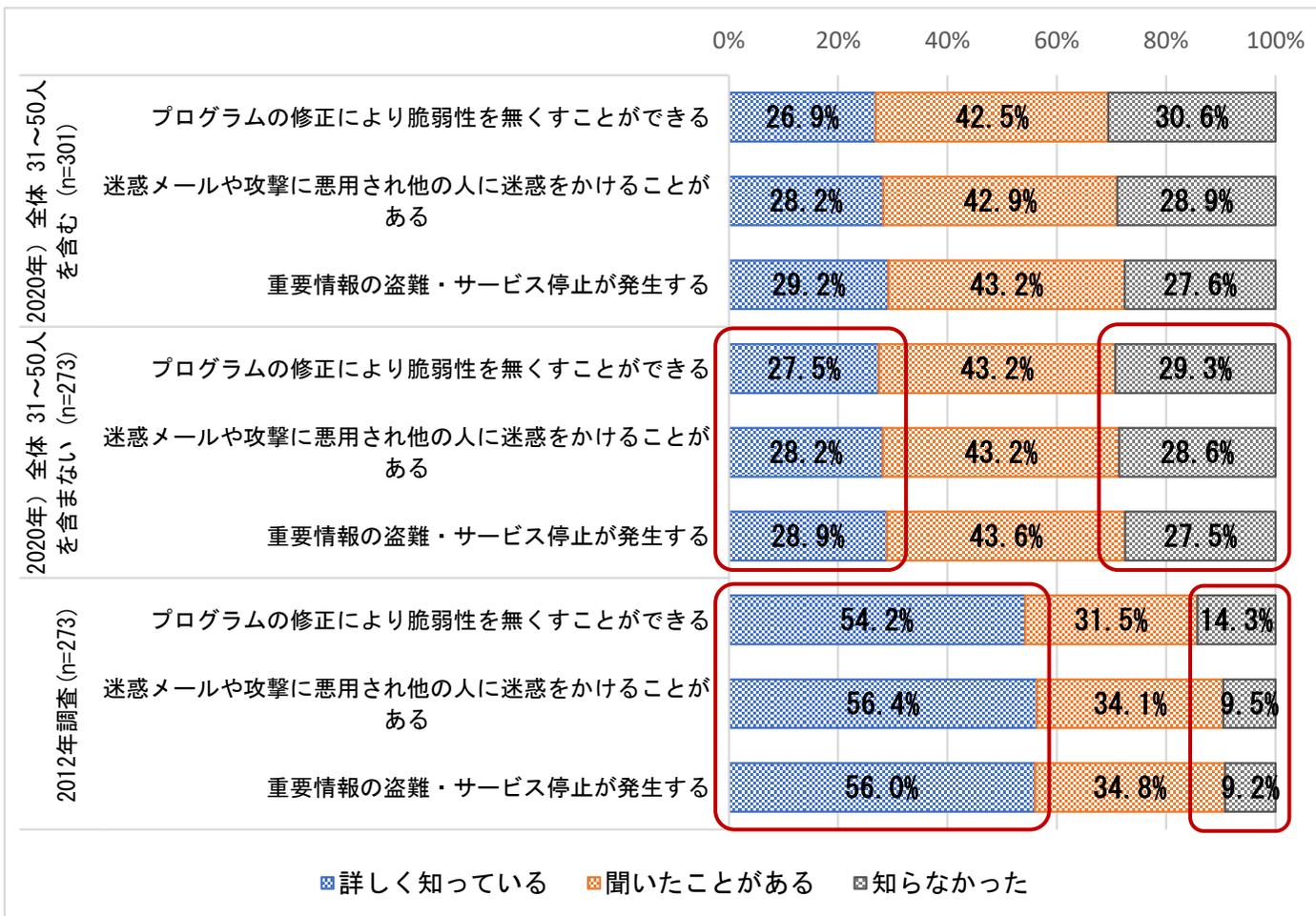
問9：ウェブサイトのセキュリティ対策の管理・組織的な体制

- 全体では、担当者がいるという回答は合わせて48.4%、「組織的には行っていない」という回答は39.1%であった。前回調査と比較し、「組織的には行っていない」という回答が低い（左図）。
- また、「大半を外部委託で実施している」、「一部を委託している」の回答は合わせて67.1%と高い。この傾向は、2012年度調査においても同様である（右図）。



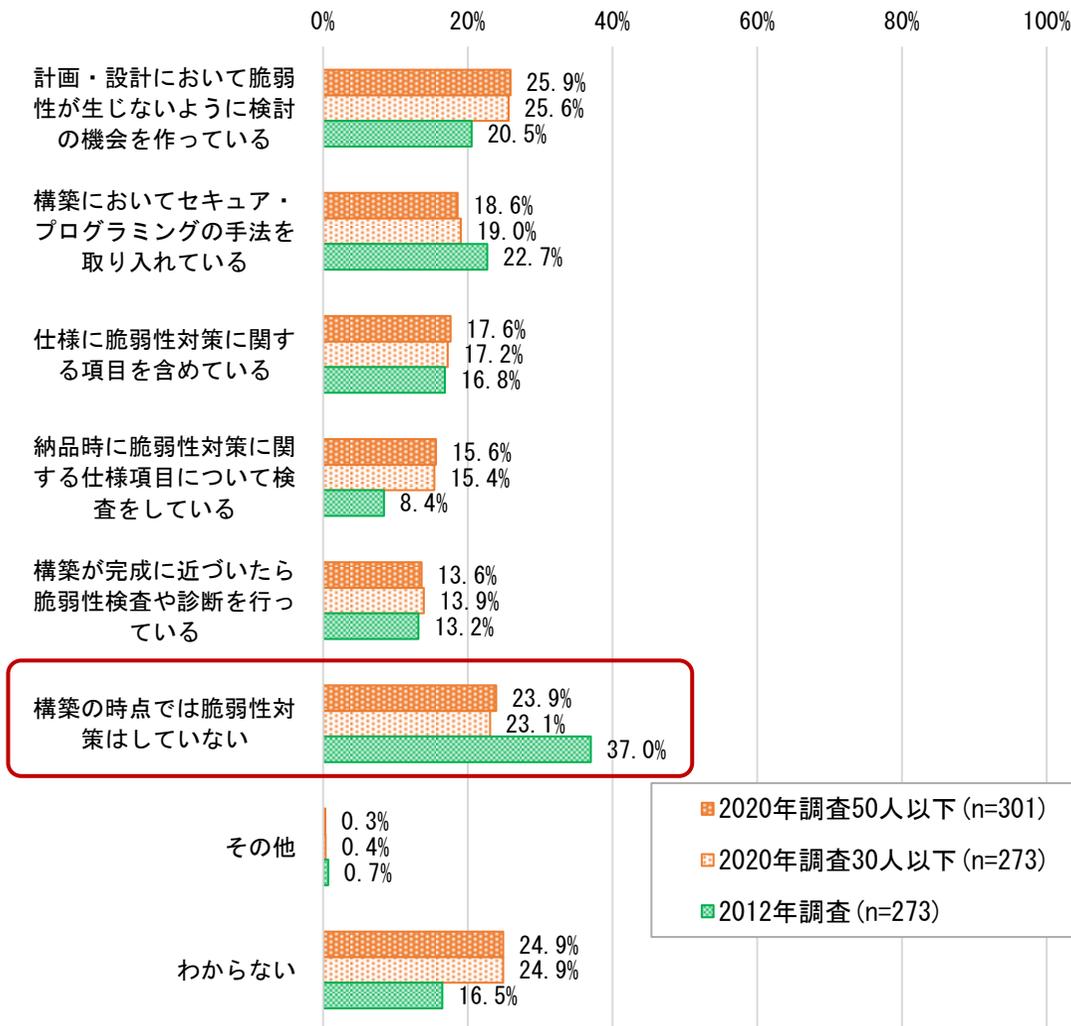
問11：ウェブサイトの脆弱性の認知度

- 全体では、約25%から30%は、「詳しく知っている」と回答し、約40%が「聞いたことがある」という回答。
- ウェブサイトの脆弱性は、前回調査に比べ、「詳しく知っている」が低下している。



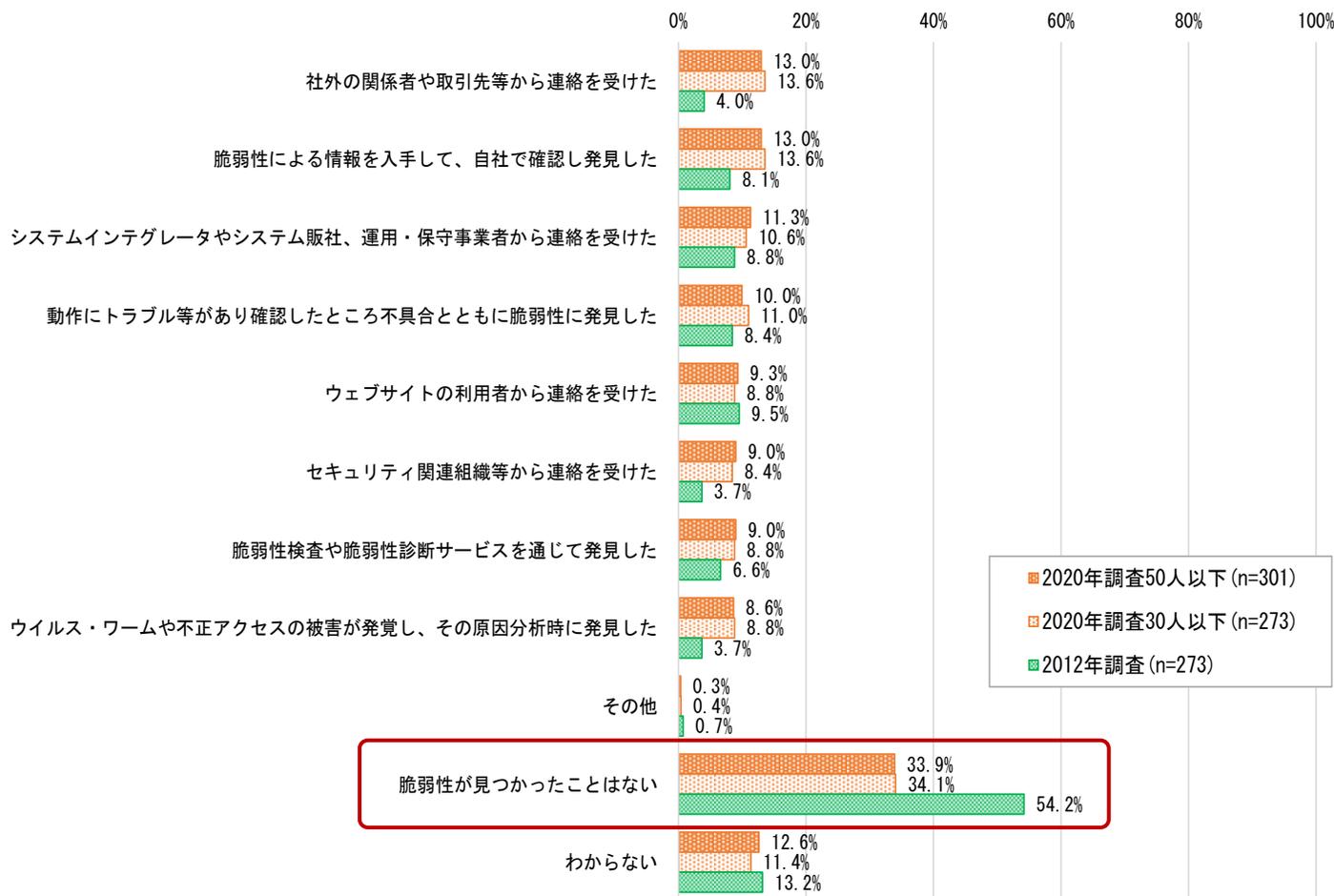
問17：ウェブサイト構築時に実施している脆弱性対策

- 全体として、「計画・設計において脆弱性が生じないように検討の機会を作っている」が25.9%と最も多く、次いで、「構築においてセキュア・プログラミングの手法を取り入れている」が18.6%であった。
- 前回調査においても同じ脆弱性対策の実施が多い傾向がある。
- 前回調査では、「構築の時点では脆弱性対策をしていない」という回答は37.0%であり、構築の時点では脆弱性対策が進んでいる傾向にある。



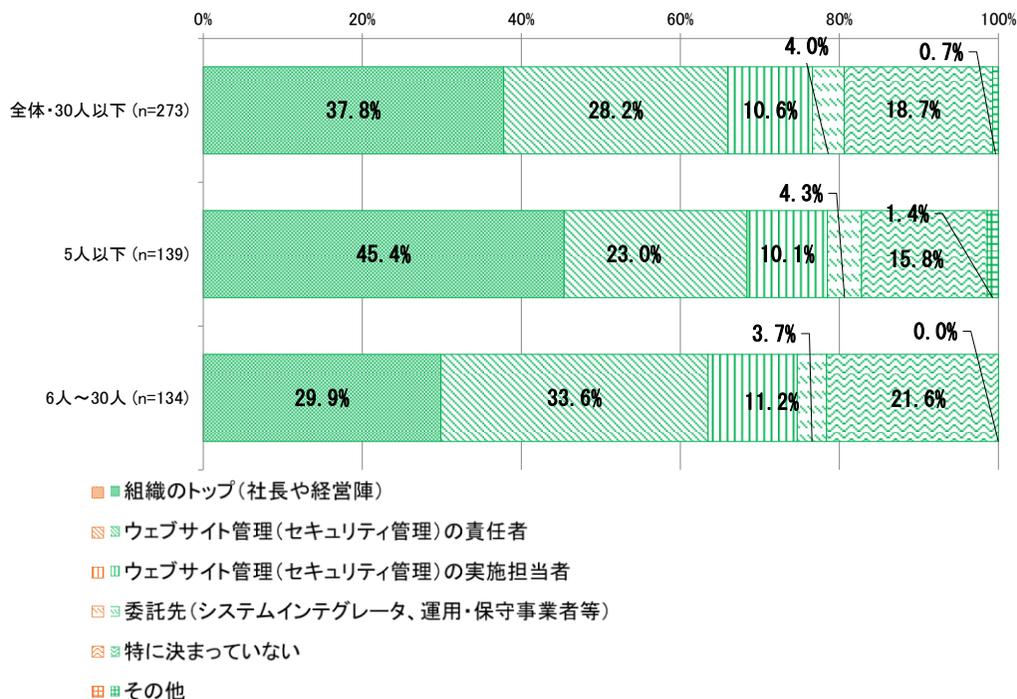
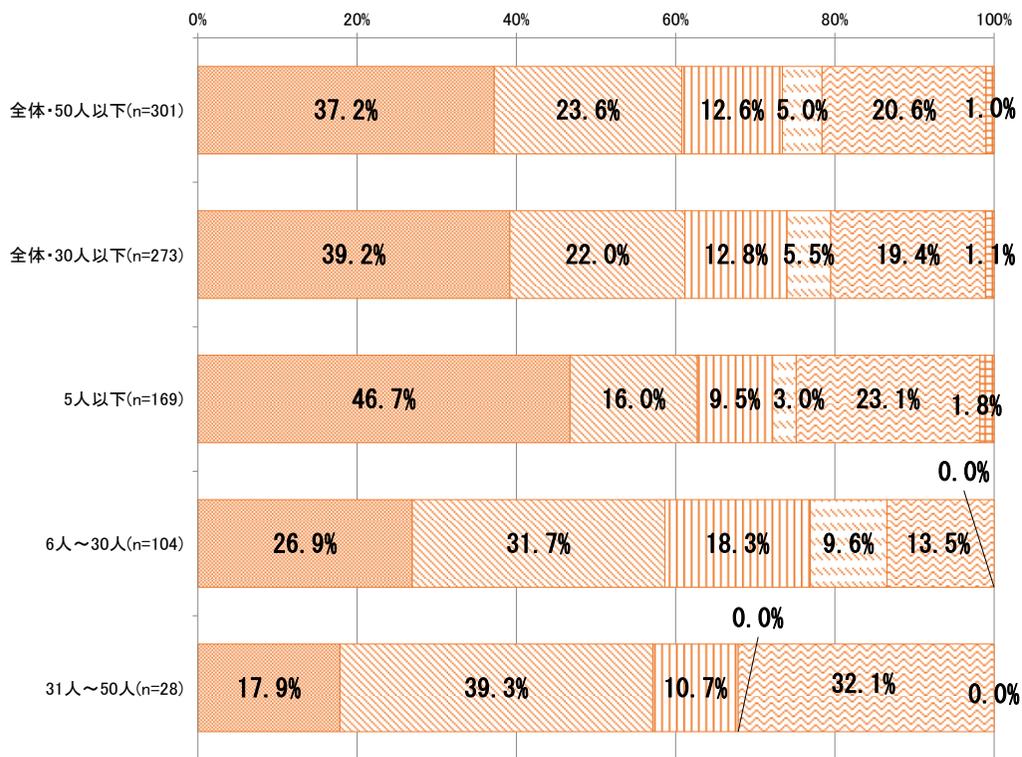
問21：運用中のウェブサイト脆弱性対策が必要だったきっかけ

- 全体では、「社外の関係者や取引先等から連絡を受けた」、「ウェブサイトの利用者から連絡を受けた」、「セキュリティ関連組織等から連絡を受けた」など組織外からの連絡を受けたことをきっかけとした回答は合わせて31.3%であった。
- 「脆弱性が見つかったことがない」は、前回調査と比較し、低くなっている。



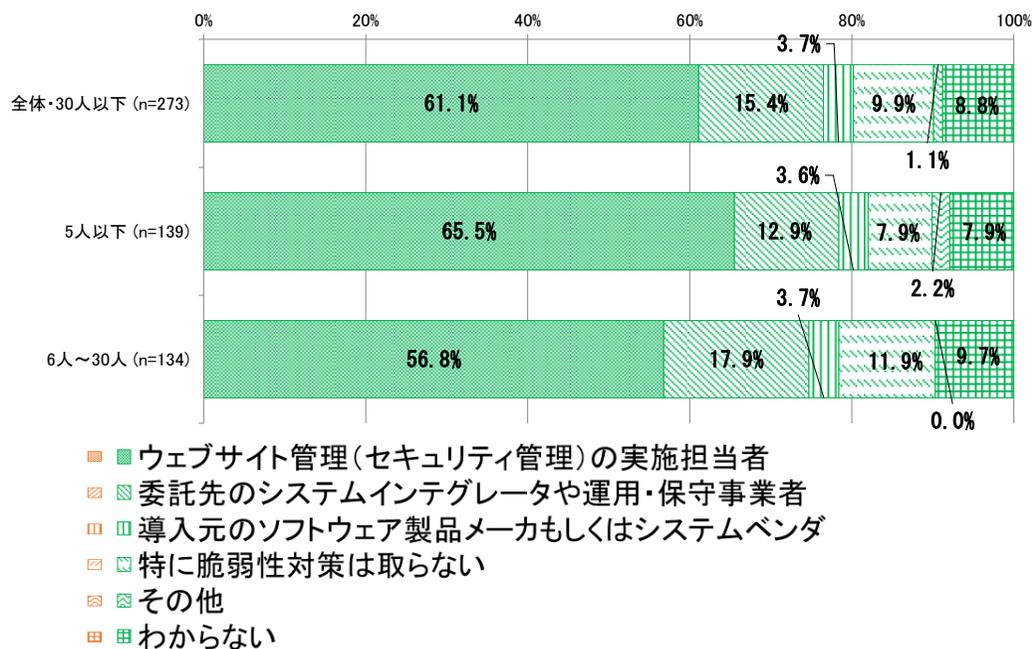
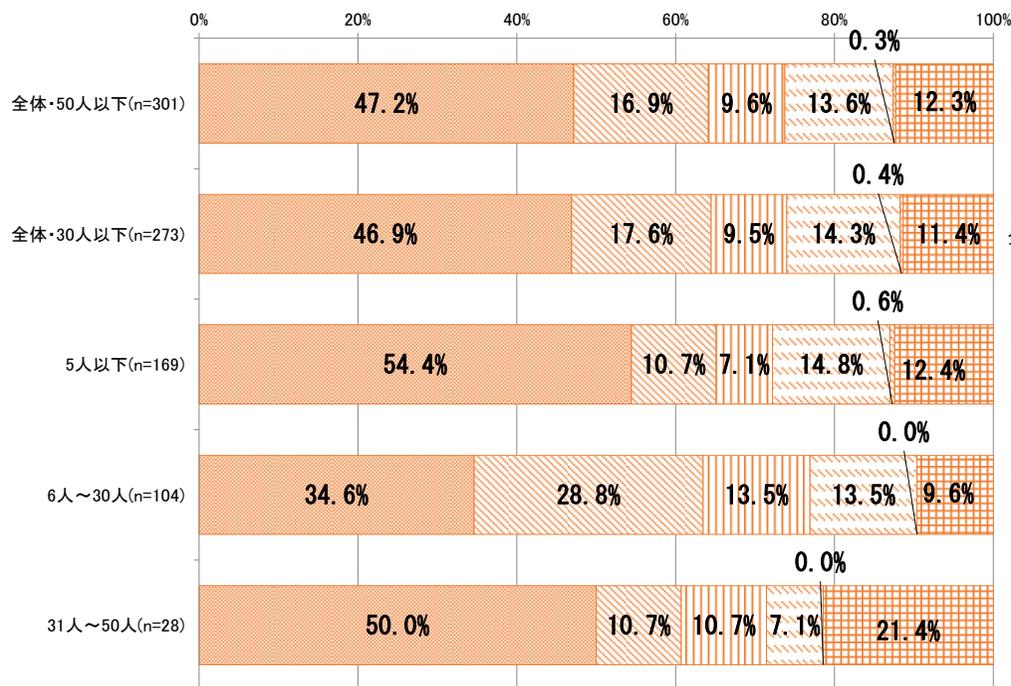
問22：ウェブサイトの脆弱性対策などの適用を判断する人

- 全体では、「組織のトップ」が37.2%と最も多く、次いで「ウェブサイト管理の責任者」が23.6%、「特に決まっていない」が20.6%であった。
- 従業員5人以下は、他に比べ組織のトップが著しく多い。従業員31人～50人は他に比べ特に決まっていないが多い。
- 前回調査と比較すると、全体では回答の多い順は「組織のトップ」、「ウェブサイト管理の責任者」、「特に決まっていない」と同傾向である。



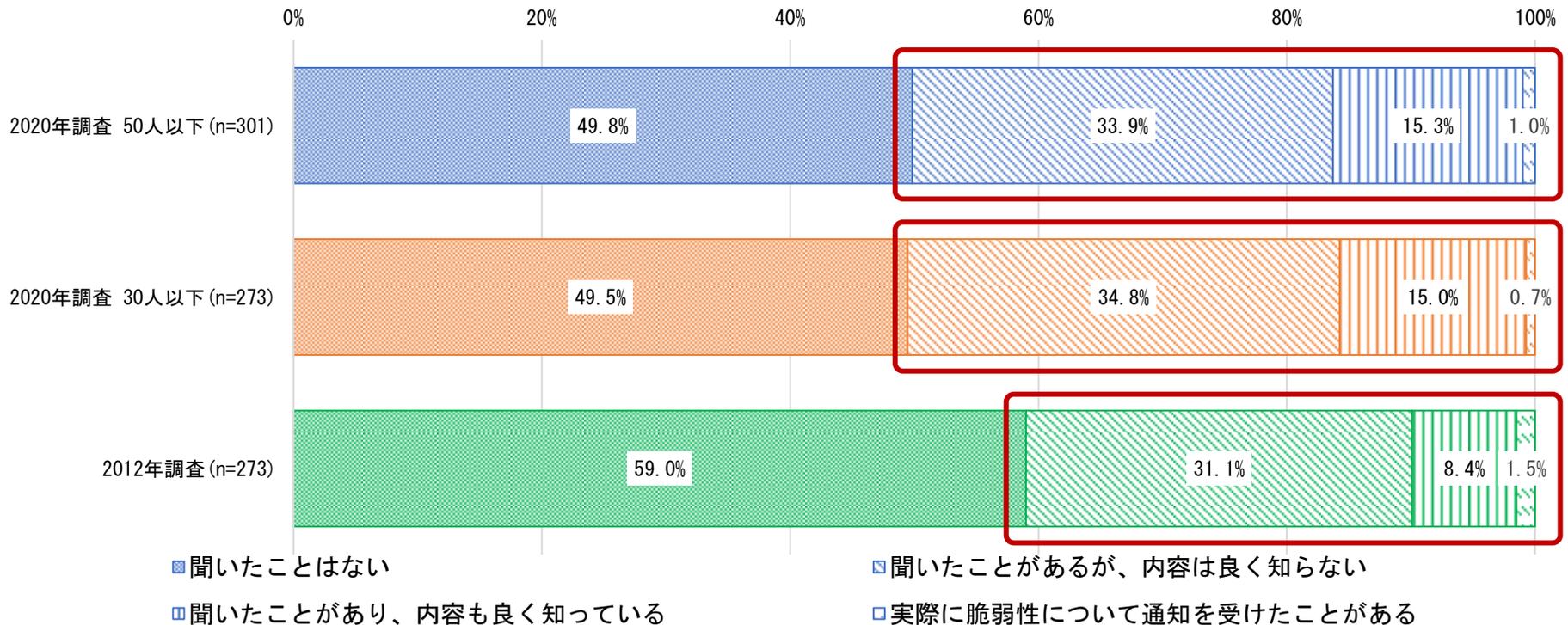
問24：運用中のウェブサイトへの一時停止・該当箇所の作業担当

- 全体では、「ウェブサイト管理の実施担当者」が47.2%と最も多く、次いで「委託先のシステムインテグレータや運用・保守事業者」が16.9%であった。
- 前回調査結果と比較すると、全体では回答の多い順は「組織のトップ」、「ウェブサイト管理の責任者」、「特に決まっていない」と同傾向である。



問27：「情報セキュリティ早期警戒パートナーシップ」の認知度

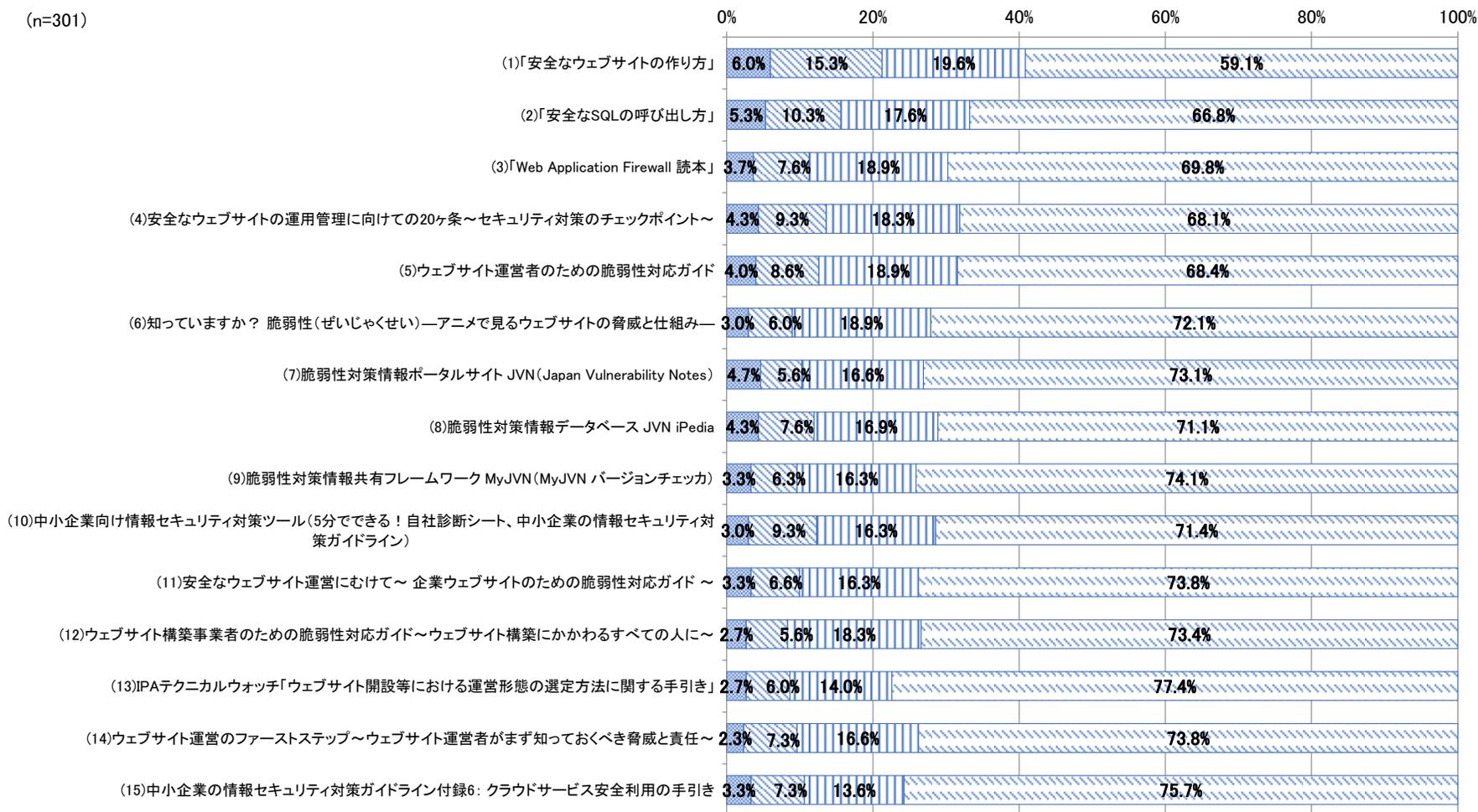
- 聞いたことがあるとする回答は合わせて約50%であり、前回調査の約40%に比べ多い。



問28：脆弱性対策・セキュリティ対策に関する認知度

- 全体では、最も知られているものは「安全なウェブサイトの作り方」であり、40.9%であった。
- また、「聞いたことはない」とする回答は、すべての情報において約60%から70%であった。

(n=301)



参考になっている
 読んだ(見た)ことはある
 聞いたことはあるが、内容は知らない
 聞いたことはない

問28：脆弱性対策・セキュリティ対策の認知度（2012年度調査結果）

- 2012年度調査においても同様の傾向があり、最も知られているものは「安全なウェブサイトの作り方」であり、36.2%であった。
- また、「聞いたことはない」とする回答は、すべての情報において約60%から80%であった。

