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

2021 年 3 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目　次

1.調査概要

1.1. 調査目的

IPA では、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、情報セキュリティ早期警戒パートナーシップ（以下、パートナーシップとする）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。

このような背景のもと、ウェブサイトでの適切な脆弱性対処の実現をめざすため、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った。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検討した。

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」として取り纏めた。また、これらの結果は、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」の改訂の要否及び改訂の内容を検討するにあたって参考とし、その改訂する内容が本調査で抽出できた課題の解消に資するものとなるようにした。

1.2. 調査手法

小規模ウェブサイトの運営およびセキュリティ対策、特に脆弱性対策の実態を把握するため、企業モニターを対象に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 担当者等に対してプレ調査を行い、回答者の中からウェブサイト運営に関与する者を抽出した上で本調査にあたっている。詳細については後述する。

2.「企業のウェブサイト運営に関する実態」アンケート調査

2.1. 調査の概要

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 担当者等に対してプレ調査を行い、回答者の中からウェブサイト運営に関与する者を抽出した上で本調査にあたっている。

項目	内容
調査方法	ウェブアンケート調査（企業モニター）
調査対象	・ 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
有効回収数	301 件（本調査）
調査実施期間	2020 年 12 月

※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。

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。

2.2. 調査項目

アンケート調査の主な設問項目は以下の通りである。

＜アンケート プレ調査の設問項目＞

（１）回答者および所属する企業等の基本属性
（２）ウェブサイトに係る業務への関与
（３）ウェブサイトの特徴

＜アンケート 本調査の設問項目＞

（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）

2.3.調査分析の方針

アンケート調査に関しては、14 項目の調査仮説を立てて調査にあたった。以下に示すように質問を設定してこれらの仮説の検証にあてることとした。

(1) ウェブサイトの構築・運用の実態について

(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 問 9 「ウェブサイトにトラブルが生じたとき、どのように関与しますか」

→ 本調査 問 9 「貴社のウェブサイトのセキュリティ対策の管理は組織的に行っていますか」

→ 本調査 問 25 「ウェブサイトの脆弱性対策・セキュリティ対策に必要な費用や人員はどの程度確保されていますか」

(仮説 2) 構築および運用の方針は経営者が決定

→ 本調査 問 5 「ウェブサイトの運用・構築について、貴社のトップ（社長や経営陣）はどのように関与していますか。」

→ 本調査 問 22 「ウェブサイトの脆弱性対策などのセキュリティ対策について、対策を適用すべきか否か等を判断する人は誰ですか」

(仮説 3) セキュリティ対策は運用段階の対策を実施している

→ 本調査 問 17 「ウェブサイトを構築する際に、どのような脆弱性対策を実施していますか」

→ 本調査 問 19 「ウェブサイトを運用する際に、どのような脆弱性対策を実施していますか」

(2) 脆弱性対策への理解について

(仮説 4) 脅威を認識しておらず危機感がない（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）

→ 予備調査 問 10 「ウェブサイトにはどのような機能・画面がありますか」

→ 本調査 問 11 「ウェブサイトの脆弱性について、どの程度知っていましたか」

→ 本調査 問 12 「国内のウェブサイトへの脆弱性を悪用した攻撃などによって企業や組織が被害を受けていることを知った時にどうしていますか」

→ 本調査 問 20 「脆弱性対策を行わない理由を教えてください」

(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 問 11 「ウェブサイトの脆弱性について、どの程度知っていましたか」

→ 本調査 問 20 「脆弱性対策を行わない理由を教えてください」

(3) 脆弱性対策の現状と課題について

(仮説 6) ウェブサイトを一時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 問 26(6) 「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：脆弱性を修正すると、ウェブ上のアプリケーションが動かなくなる可能性がある」

→ 本調査 問 26(8) 「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：脆弱性の問題でサービスを止めると、顧客を失ってしまう」

→ 本調査 問 26(9) 「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：脆弱性対策やセキュリティ対策について組織トップの理解を得ることが難しい」

(仮説 7) ウェブサイトのセキュリティ対策へ費やす予算や人手が十分ではない

→ 本調査 問 25 「ウェブサイトの脆弱性対策・セキュリティ対策に必要な費用や人員はどの程度確保されていますか」

→ 本調査 問 26(1) 「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：対策を行うための予算が確保できない」

→ 本調査 問 26(3) 「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：対策を行うための人員が足りない」

(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 問 8 「貴社のウェブサイトの運用・構築を担当する方（ウェブサイト担当者）はどのような理由で選ばれていますか」

→ 本調査 問 26(2)「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：脆弱性やセキュリティに関する技術の習得が難しい」

(仮説 9) トラブルが生じても脆弱性対策による根本的な解決は行われない

→ 本調査 問 19 「ウェブサイトを運用するにあたり、どのような脆弱性対策を実施していますか」

→ 本調査 問 23 「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はありますか」

→ 本調査 問 24 「もし運用中のウェブサイトについて脆弱性が発見された場合には、ウェブサイトの一時停止、該当箇所の修正、回避策の適用等（含テスト）の作業は誰が担当しますか」

(4) IPA の普及啓発資料に関する認知度について

(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 問 27 「情報セキュリティ早期警戒パートナーシップの取組みについて知っていますか」

→ 本調査 問 28 「脆弱性対策・セキュリティ対策に関する次の情報について知っていますか」

(5) ウェブサイトの対策・重要性の変化

(仮説 11) 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 問 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」

→ 本調査 問 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」

(仮説 12) 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けるコストは変わらない

→ 本調査 問 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」

→ 本調査 問 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」

→ 本調査 問 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」

→ 本調査 問 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」

(6) クラウド利用対策及び複数・複合的な対策

(仮説 13) 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 問 4「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」

(仮説 14) 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 問 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」

2.4. 調査結果

2.4.1. 回答企業および回答者について

(1) 従業員数

回答者の所属する企業等の従業員数については「1～5 人」(56.1%) が最も多く、「6～10 人」、「31～50 人」(9.3%)、「16～20 人」(8.0%) が続く。2012 年度調査では、「1～5 人」が最も多く、「6～10 人」、「16～20 人」が続く。「31～50 人」を除き同じ傾向であったが、2012 年度調査に比べ、「6～10 人」が少ない。

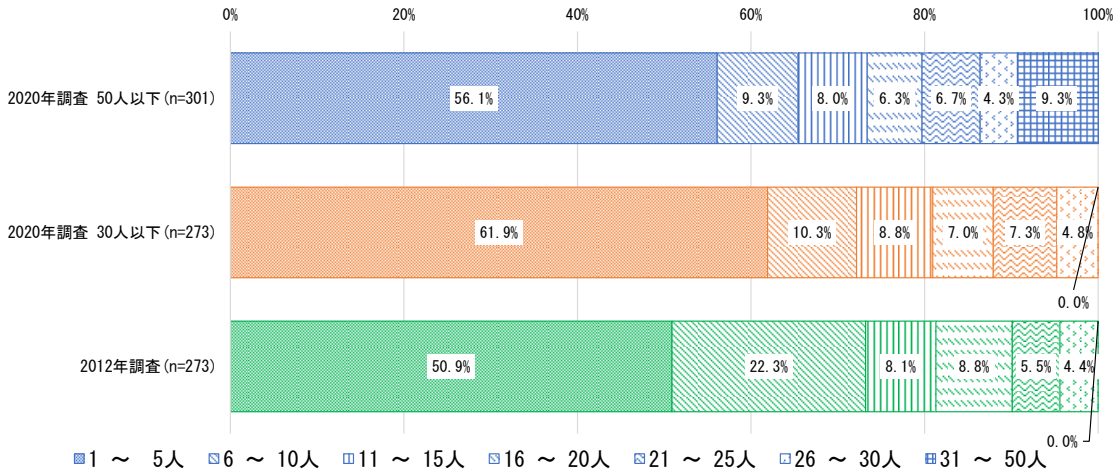

図 2.4.1 回答者の所属する企業等の従業員数（予備調査 問 1）

(2) 業種

回答者の所属する企業等の業種については「その他のサービス」(35.2%) が最も多く、「情報通信、IT 関連サービス」(29.2%)、「卸売」(5.0%)、「小売」(4.7%) が続く。2012 年度調査では、「その他のサービス」が最も多く、「情報通信、IT 関連サービス」、「小売」、「製造」という順であり、「その他のサービス」、「情報通信、IT 関連サービス」、「小売」が共通して多い。

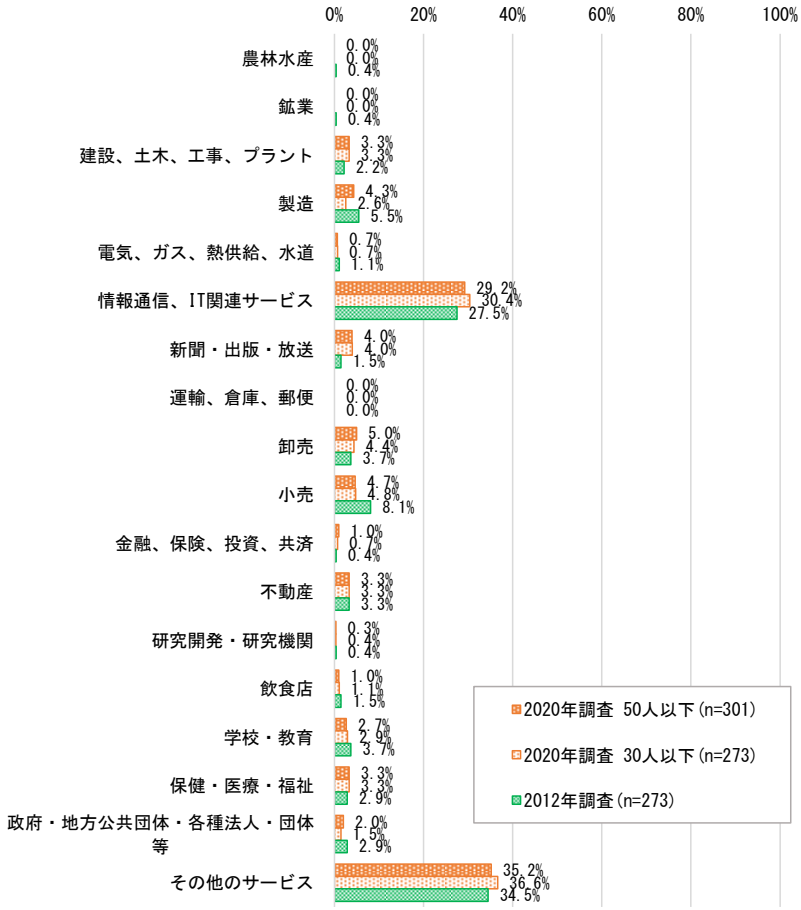

図 2.4.2 回答者の所属する企業等の業種（予備調査 問 2）

(3) 所在地

回答者の所属する企業等の所在地については「首都圏」が 36.2%、「地方（人口 30 万人以上)」が 45.8%、「地方（人口 30 万人未満)」が 17.9%であった。2012 年度調査では、「首都圏」が 42.2%、「地方（人口 30 万人以上)」が 41.0%、「地方（人口 30 万人未満)」が 16.8%であった。

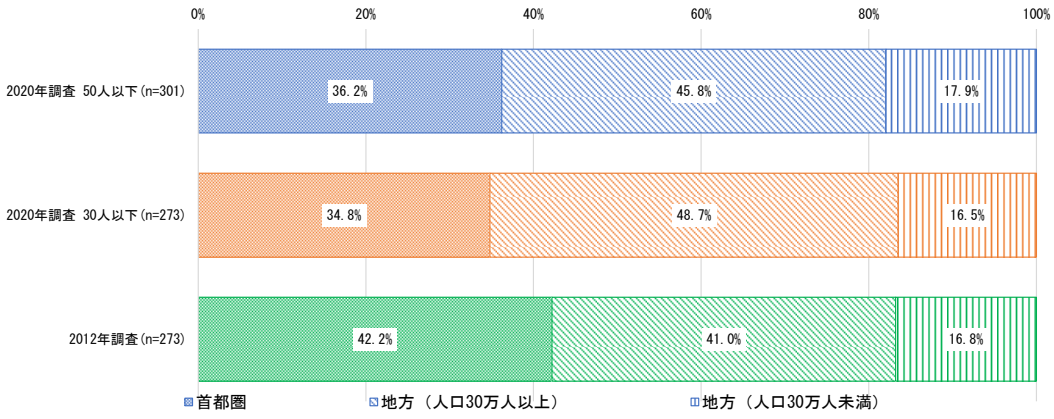

図 2.4.3 回答者の所属する企業等の所在地（予備調査 問 3）

(4) 回答者が担当する業務

回答者としてウェブサイトに関与する者を抽出するため、予備調査で回答者が担当する業務を質問し、その答えで本調査対象者を絞り込んだ。回答者の業務は「Web サイト構築・管理」（29.9%）、「顧客サービス・サポート、顧客管理」（23.9%）、「コンテンツ企画・制作」（23.3%）、「広報・宣伝」（15.3%）、「社内向けシステム・情報システム企画運用管理」（7.6%）であった。2012 年度調査に比べ、「Web サイト構築・管理」が少なく、「コンテンツ企画、制作」が高い傾向にある。

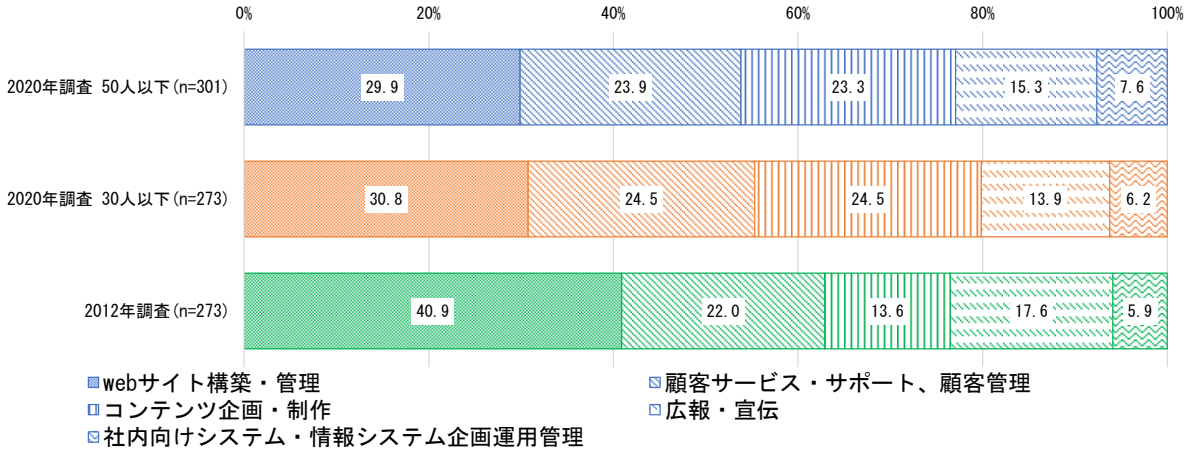

図 2.4.4 回答者が担当する業務（予備調査 問 11）

2.4.2.回答者とウェブサイトの関わりについて

(1) 職務で関わっているウェブサイトの範囲

回答者が職務で関わっているウェブサイトが自社のものであるか、他社（顧客）のものであるかを尋ねた。「自社のウェブサイトのみに関わっている」が 59.5%と最も多く、次いで「他社（顧客）のウェブサイトに関わっている」が 25.2%と多い。また、2012 年度調査に比べ、「自社と他社（顧客）のウェブサイトの両方に関わっている」が少なく、「他社（顧客）のウェブサイトに関わっている」が多い傾向にある。

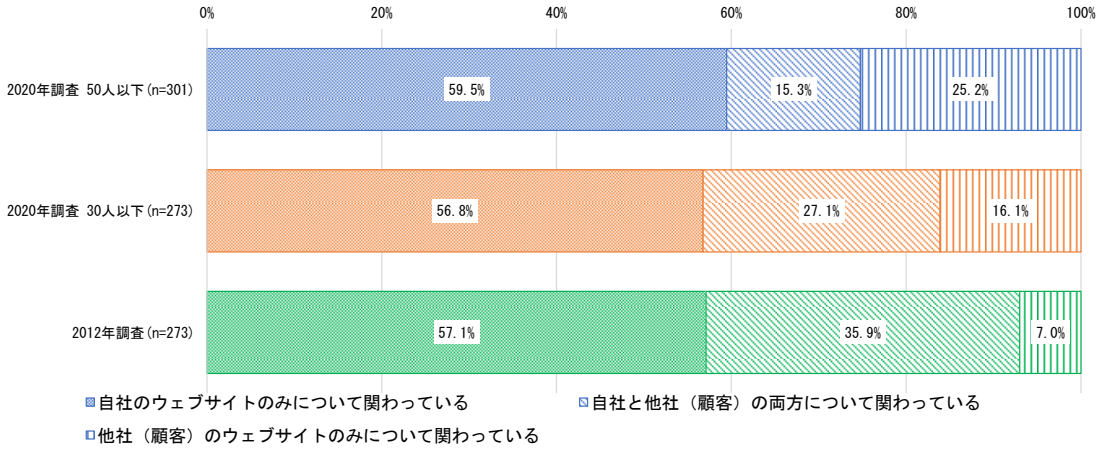

図 2.4.5 職務で関わっているウェブサイトの範囲（予備調査 問 4）

(2) 自社ウェブサイトに関する回答者の業務

自社ウェブサイトに関与している回答者に対して、どのような業務に関わっているかを複数回答可で尋ねたところ、「自社ウェブサイトの保守・運用・監視」(50.2%)、「自社ウェブコンテンツの企画・制作」(48.2%)、「自社ウェブサイトの構築（外注を含まない）」(41.6%)、「自社ウェブサイトを用いた広報・宣伝」(32.2%)、「自社ウェブサイトの企画・発注（外注管理を含む）」（32.2%）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が、2012 年度調査に比べ、上記の回答はすべて低下している。

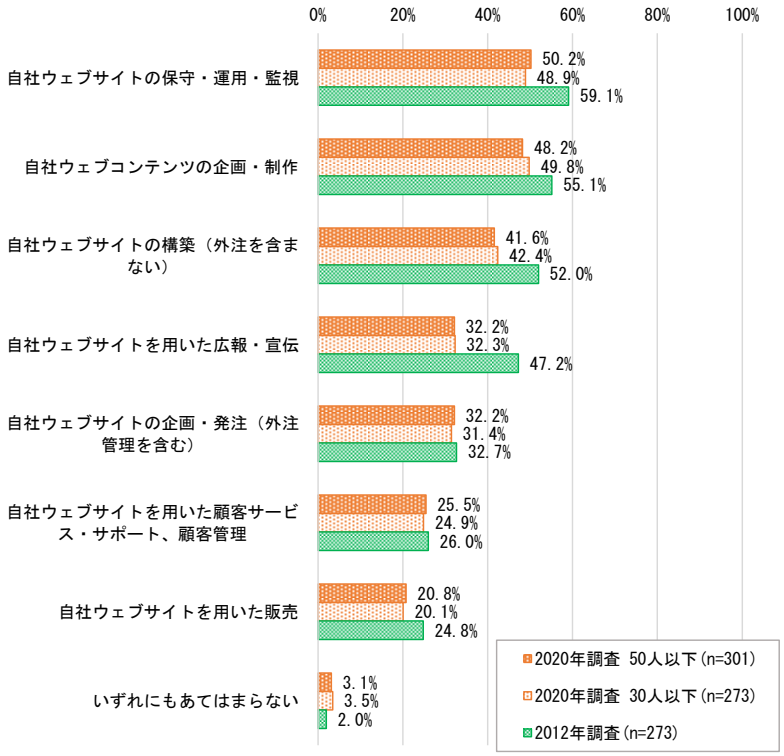

図 2.4.6 自社ウェブサイトに関する回答者の業務（予備調査 問5）

(3) 顧客ウェブサイトに関する回答者の業務

他社（顧客）のウェブサイトに関与している回答者に対して、どのような業務に関わっているかを複数回答可で尋ねた。「他社（顧客）のウェブコンテンツの企画・制作」が最も多く（64.8%）、「他社（顧客）のウェブサイトの構築」、「他社（顧客）のウェブサイトの保守・運用・監視」もそれぞれ60%を超えた。この傾向は、2012年度調査においても同様である。

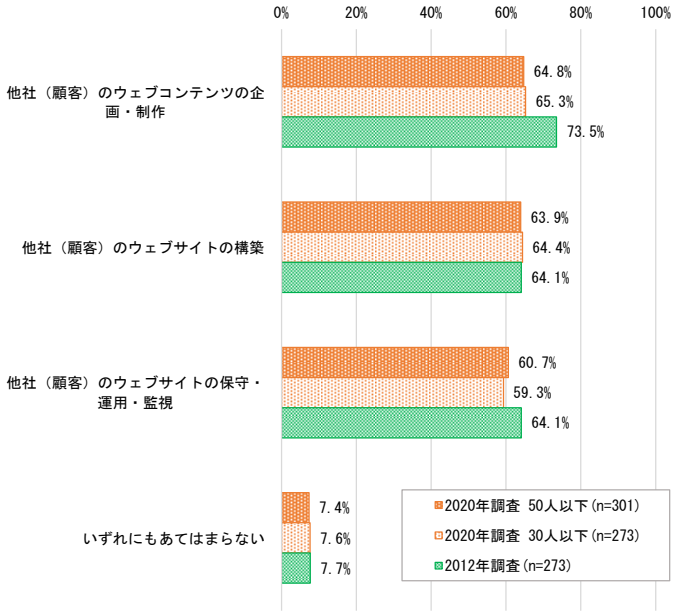

図 2.4.7 顧客ウェブサイトに関する回答者の業務（予備調査 問 7）

(4)ウェブサイトにトラブルが発生した際の回答者の関与

ウェブサイトでトラブルが発生した場合に回答者がどの程度関与しうるかについて尋ねた。「主にあなた自身がトラブルに対処する」と答えた回答者が 44.5%と最も多い。また、2012 年度調査についても同様の傾向である。

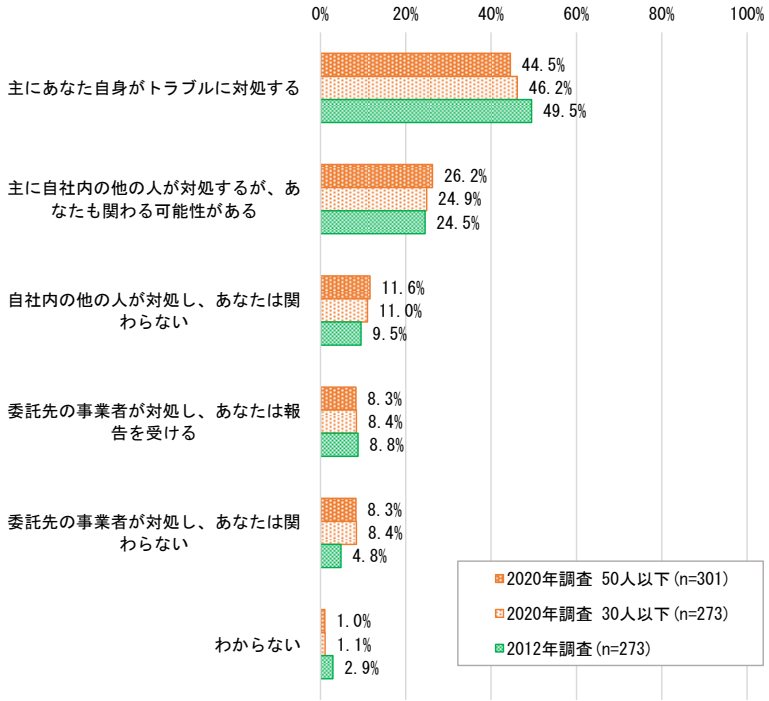

図 2.4.8 ウェブサイトでトラブルが発生した際の回答者の関与（予備調査 問 9）

2.4.3. ウェブサイトについて

(1) 自社ウェブサイトの特徴

自社のウェブサイトの特徴についてあてはまるものを質問した（複数回答可）。「製品・サービスの案内」(63.1%)、「企業案内」(61.6%)、「問い合わせ受付」(53.7%）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。

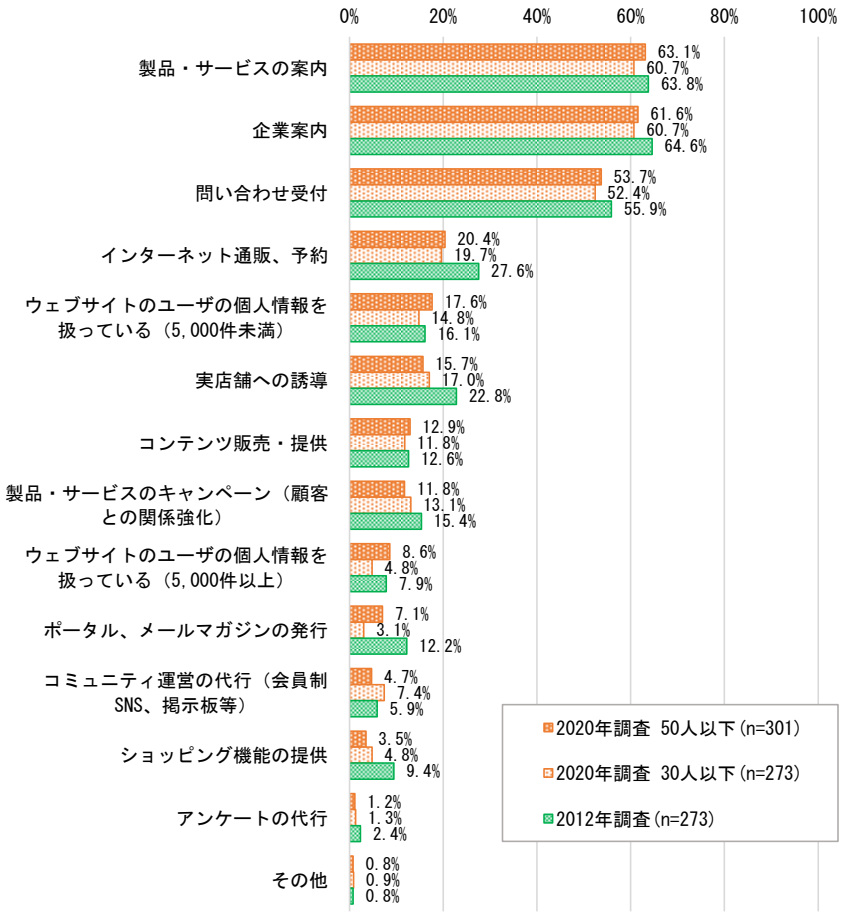

図 2.4.9 自社ウェブサイトの特徴（予備調査 問 6）

(2) 顧客ウェブサイトの特徴

取り扱っている他社（顧客）のウェブサイトの特徴についてあてはまるものを質問した（複数回答可）。「製品・サービスの案内」(68.0%)、「企業案内」(65.6%)、「問い合わせ受付」(45.9%）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。

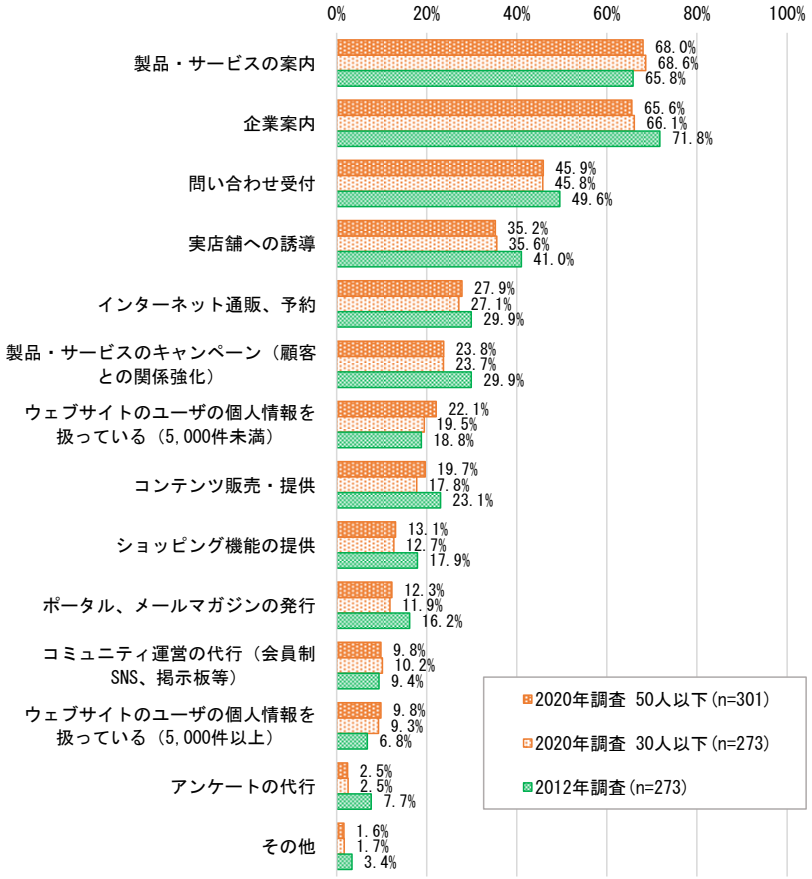

図 2.4.10 顧客ウェブサイトの特徴（予備調査 問 8）

(3) ウェブサイトが備える機能・画面

取り扱うウェブサイトが備える機能・画面について質問した（複数回答可）。選択肢は「安全なウェブサイトの作り方[1]」に示される「注意が必要なウェブサイトの特徴」を参考に脆弱性を作りこむ可能性がある機能・画面を設定した。「ユーザによるフォームの入力（問合せ、掲示板等を含む）」(56.5%)、「サイト内の検索と結果表示」(36.9%)、「ユーザへのメールの自動送信」(36.9%)、「入力された情報の確認のための表示」(34.6%) 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。

[1] 「安全なウェブサイトの作り方」 https://www.ipa.go.jp/security/vuln/websecurity.html

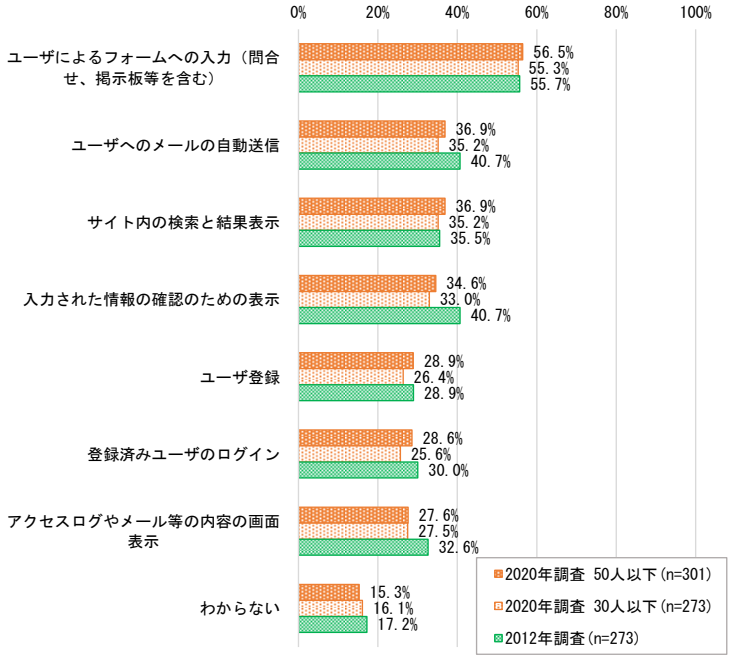

図 2.4.11 ウェブサイトが備える機能・画面（予備調査 問 10）

(4)ウェブサイトの構築後の年数

ウェブサイトの構築後の年数について質問した。全体では「10 年以上」（35.9%）、「5 年以上～10 年未満」（26.9%）、「1 年以上～5 年未満」（23.6%）が上位を占めた。この傾向は、従業員数の規模別においても同様であるが、従業員数 31 人～50 人の組織は、「10 年以上」（42.9%）が他に比べ若干多い傾向がある。

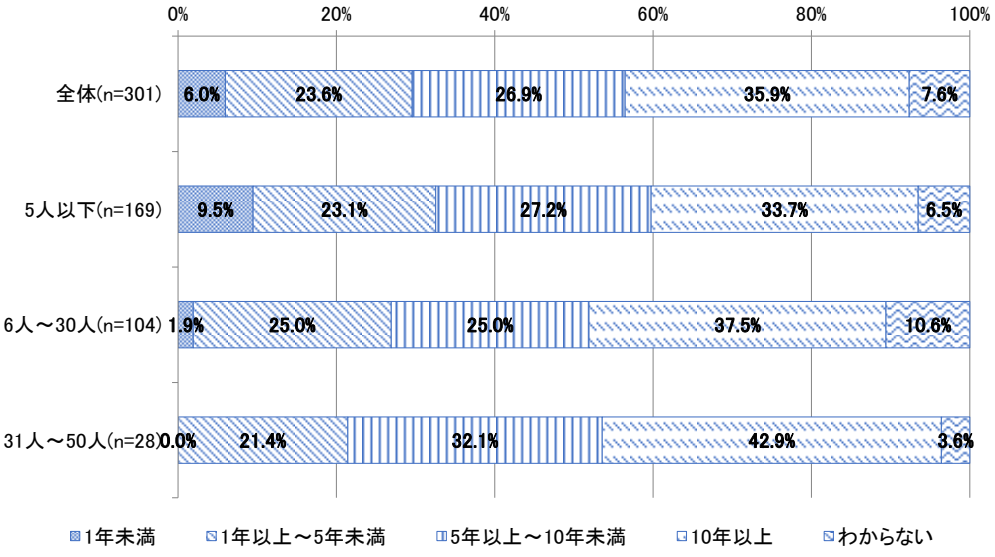

図 2.4.12 ウェブサイトの構築後の年数（本調査 問 7）

(5)ウェブサイトの開発・構築

(a) 開発・構築の方法

ウェブサイトの開発・構築の方法を質問した。全体では、自社で開発・構築するという回答が多く、合計が 52.8%（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 28.9%、自社で独自にウェブアプリケーションを開発し、構築 8.0%、既存のパッケージを利用・カスタマイズし、構築 15.9%）であり、およそ過半数を占めた。

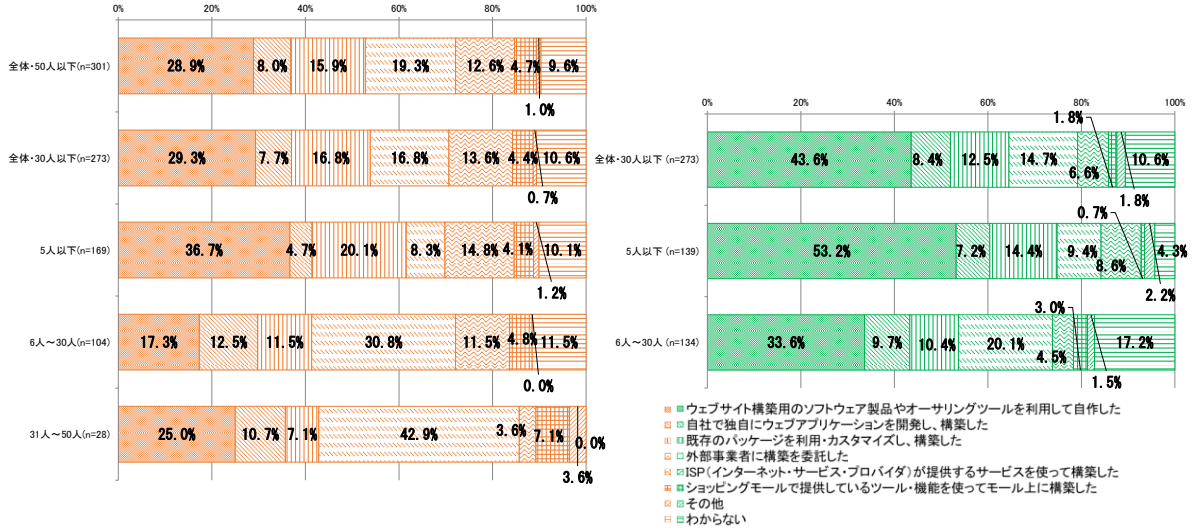

図 2.4.13 開発・構築の方法（本調査 問 1）

従業員規模別では、5 人以下の組織は「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」(36.7%）が最も多く、次いで「既存のパッケージを利用・カスタマイズし、構築」(20.1%）であった。6 人～30 人の組織及び 31 人～50 人の組織は「外部事業者に構築を委託した」(6 人～30 人の組織 30.8%、31 人～50 人の組織 42.9%）が最も多く、次いで「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」(6 人～30 人の組織 17.3%、31 人～50 人の組織 25.0%）であった。従業員規模が多くなると自社開発よりも外部事業者に構築を委託する傾向がある。

2012 年度調査と比較すると「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、2012 年度調査では 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。「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」は、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。

(b) 開発・構築の際に重視する点

ウェブサイトの開発・構築の際に重視する点を質問した（複数回答可）。「費用」(66.4%)、「運用時の利便性・拡張性」(65.1%）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が、2012 年度調査に比べ、「セキュリティ」の回答が増加した。

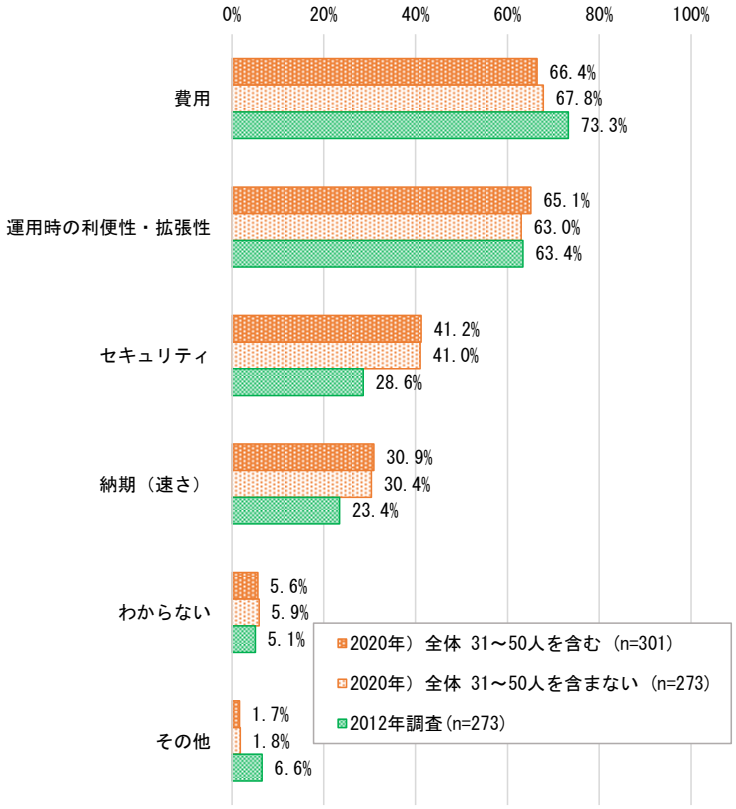

図 2.4.14 開発・構築の際に重視する点（本調査 問 2）

(6)ウェブサイトの運用・管理

(a) 運用・管理の形態

ウェブサイトの運用・管理の形態について質問した。自社内で運用・管理すると答えた回答は全体の 40.5%（自社社員が運用・管理 31.2%、委託社員が自社内で運用・管理 9.3%）であった。外部のサービスを利用しているという回答は合わせて全体の 44.5%（ホスティング 23.6%、クラウド 11.3%、ASP サービス 5.6%、ショッピングモール 4.0%）であった。従業員規模別では、「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全て運用・管理している」に関する 5 人以下の組織の回答は 29.6%、6 人～30 人の組織の回答は 30.8%であるが、31 人～50 人の組織の回答は 42.9%と他に比べて多い。

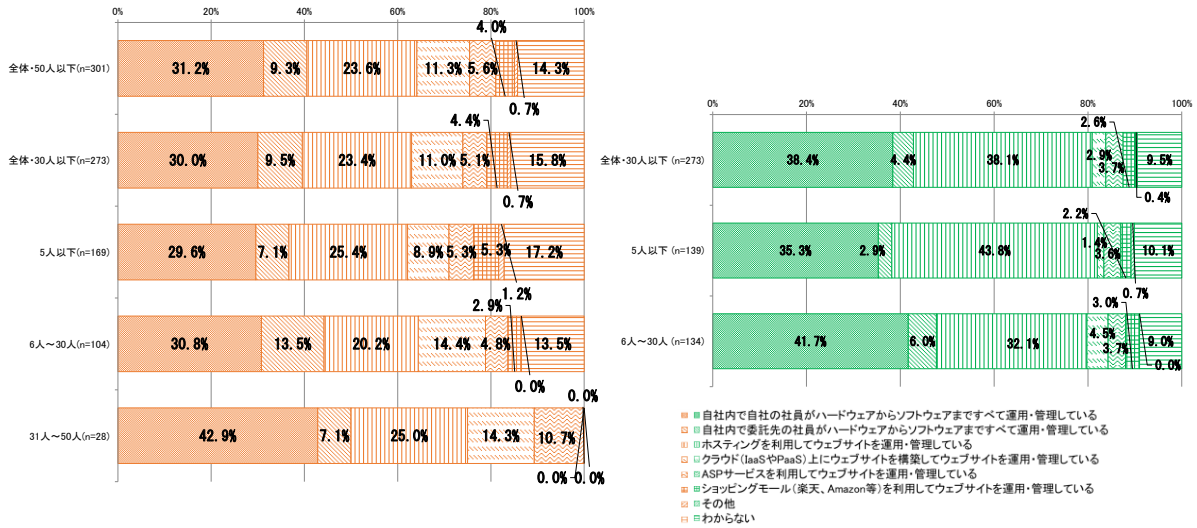

図 2.4.15 運用・管理の形態（本調査 問 3）

2012 年度調査と比較すると、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。本年度調査では、「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全て運用・管理している」（30.0%）、「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」（23.4%）、「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」（11.0%）という順であるが、2012 年度調査は「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全て運用・管理している」（38.4%）、「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」（38.1%）、「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」（2.9%）の順であった。従業員規模別でも同様の傾向がみられる。

(7) ウェブサイトに関する社内の体制

(a) 経営層の関与

ウェブサイトに関する社内の取り組みについて、トップ経営層がどの程度関与しているかを質問した。全体では「トップ自らがウェブサイトの運用・構築にあたっている」との回答が 35.5%であった。従業員規模別では、5 人以下の組織は「トップ自らがウェブサイトの運用・構築にあたっている」が 56.8%と多いが、6 人～30 人の組織、31 人～50 人の組織では、「トップ自らがウェブサイトの運用・構築にあたっている」は、10%未満であり、「積極的に担当者に指示を出し、ウェブサイトへの要望や意見も良く出している」、「ときどき担当者に指示を出し、報告も受けている」、「担当者から報告を受けているが、基本的には担当者に任せている」が 20%以上である。

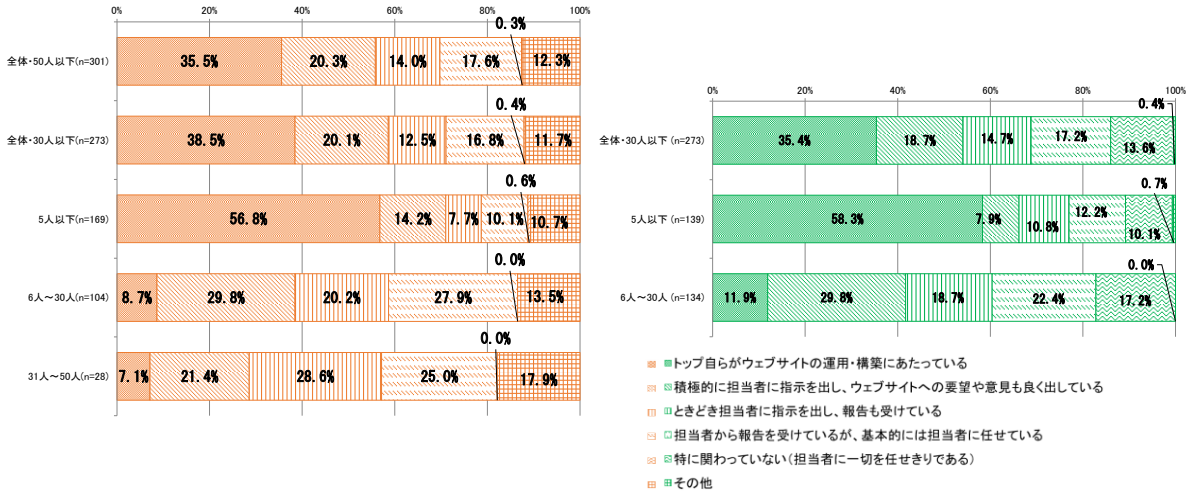

図 2.4.16 経営層の関与（本調査 問 5）

2012 年度調査との比較においても前述と同様の傾向があり、5 人以下の組織は「トップ自らがウェブサイトの運用・構築にあたっている」の回答が多く、6 人～30 人の組織（2012 年度調査、2020 年度調査双方）、31 人～50 人の組織（2020 年度調査）では、担当者に指示または報告を受けている回答が多い傾向がある。

(b)ウェブサイト担当者を選ぶ観点

ウェブサイト担当者を選ぶ視点について質問した(複数回答可)。「パソコンに慣れているから」(52.5%)、「デザインができるから」(39.5%)、「運営や管理ができるから」(37.2%) 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。

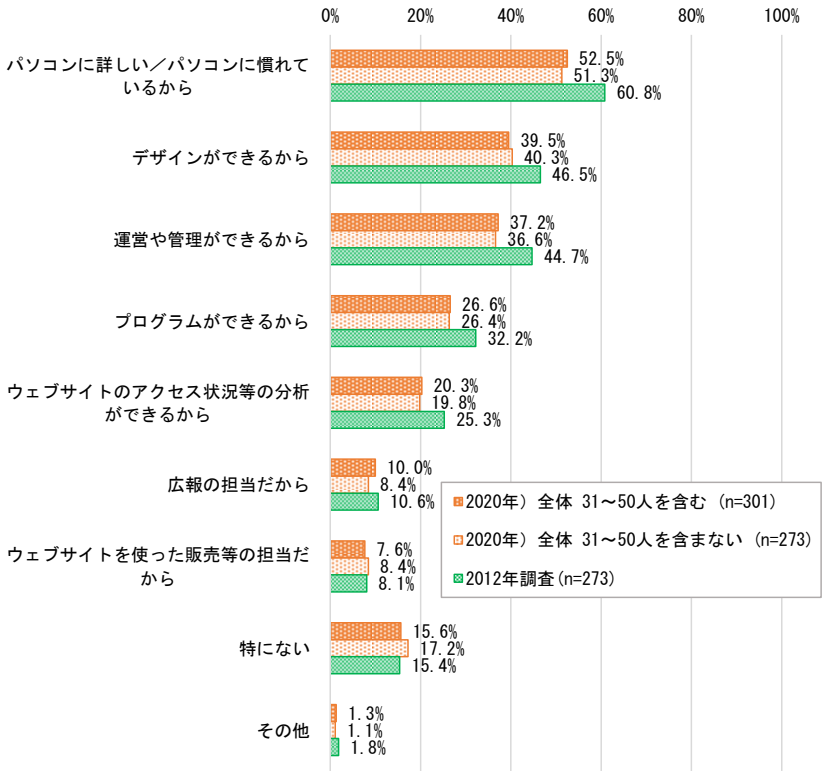

図 2.4.17 ウェブサイト担当者を選ぶ観点（本調査 問 8）

2.4.4. ウェブサイトのセキュリティ対策の状況について

(1)組織的なセキュリティ管理

ウェブサイトのセキュリティ管理について担当者を設けた組織的な管理が行われているかを質問した。担当者がいると答えた回答は全体の 48.4%（ウェブサイトのセキュリティ管理を行う当社がいる 32.7%、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 15.7%）、組織的には対応していないという回答は全体の 39.1%であった。2012 年度調査では担当者がいると答えた回答は全体の 38.1%、組織的には対応していないという回答は全体の 52.7%であり、本年度調査は 2012 年度調査に比べ、「組織的に行っていない」という回答が低い。

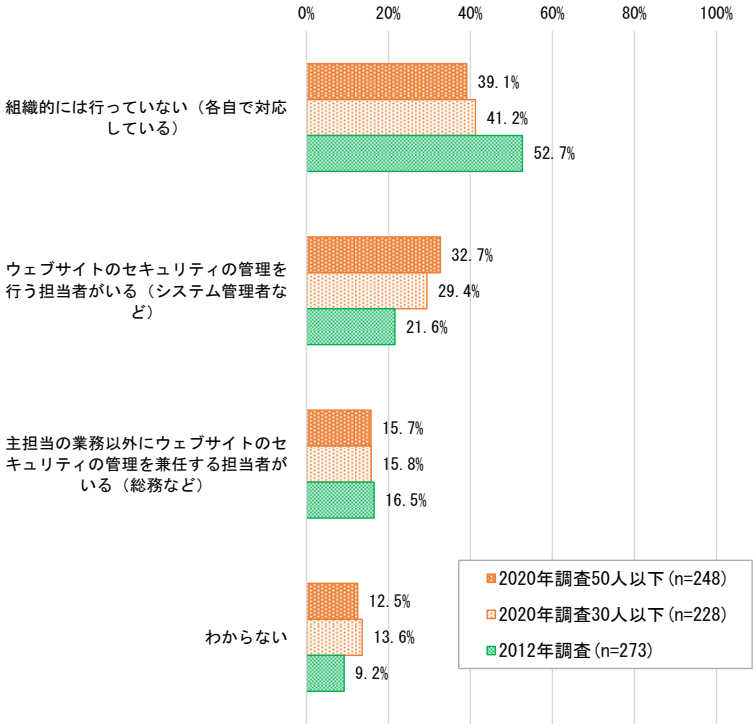

図 2.4.18 組織的なセキュリティ管理（本調査 問 9-1）

(2)セキュリティ対策の外部委託

(a)外部委託の実施

セキュリティ対策の外部委託の状況について質問した。「大半を外部委託で実施している」(39.4%)、「一部を委託している」(27.7%)の回答は合わせて 67.1%と高い。また、この傾向は、2012 年度調査においても同様である。

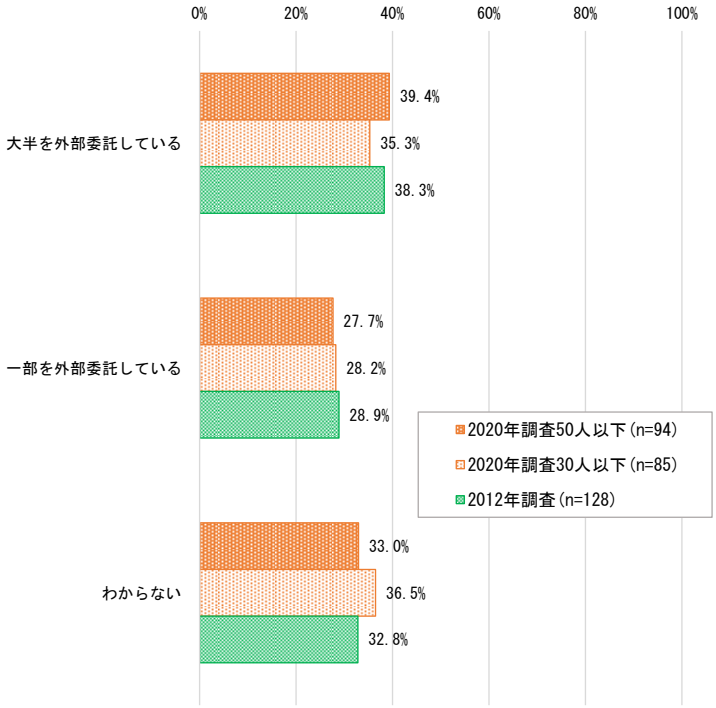

図 2.4.19 外部委託の実施（本調査 問 9-2）

(b)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の明確化

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関しての責任範囲について明確化しているかについて尋ねた。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。

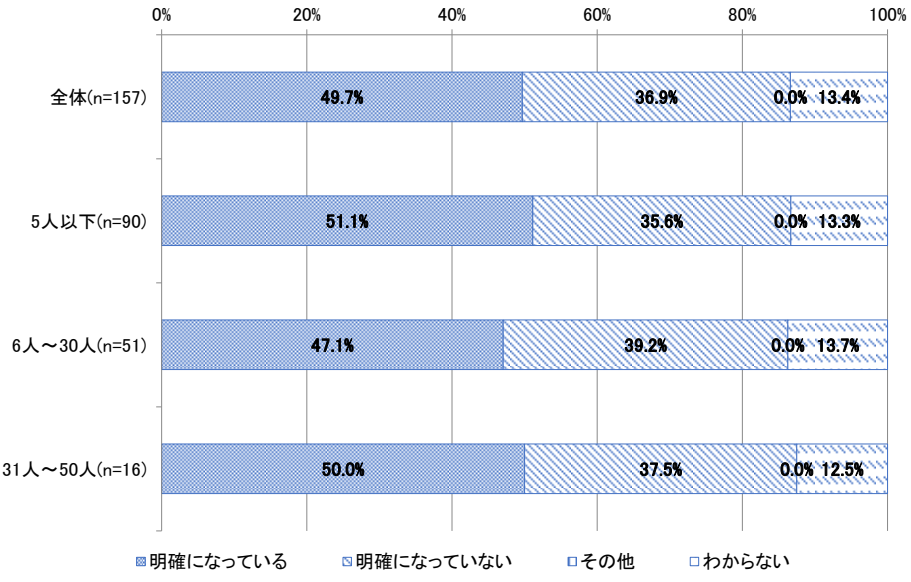

図 2.4.20 セキュリティ対策に関する自社とサービス提供者の責任範囲の明確化（本調査 問 4）

(c)セキュリティ要件

外部委託を行っていると回答した者に、委託時にセキュリティ要件をどの程度意識しているかを質問した。契約に含まれているという回答（セキュリティ要件は契約に含まれている 33.3%、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 20.6%）は合わせて 53.9%であった。契約に必須ではないという回答（セキュリティ要件は特に気にしていない 11.1%、気になるが必須ではない 15.9%）は、合わせて 27.0%であった。

従業員規模別では、5 人以下の組織は、契約に含まれているという回答が合わせて 40.9%、契約に必須ではないという回答が合わせて 36.4%であった。

6 人～30 人の組織は、契約に含まれているという回答が合わせて 62.5%、契約に必須ではないという回答が合わせて 25.0%であった。

31 人～50 人の組織は、契約に含まれているとの回答が合わせて 55.5%、契約に必須ではないとの回答が合わせて 11.1%であった。

従業員規模が多いと契約に必須ではないという回答が低下する傾向がある。

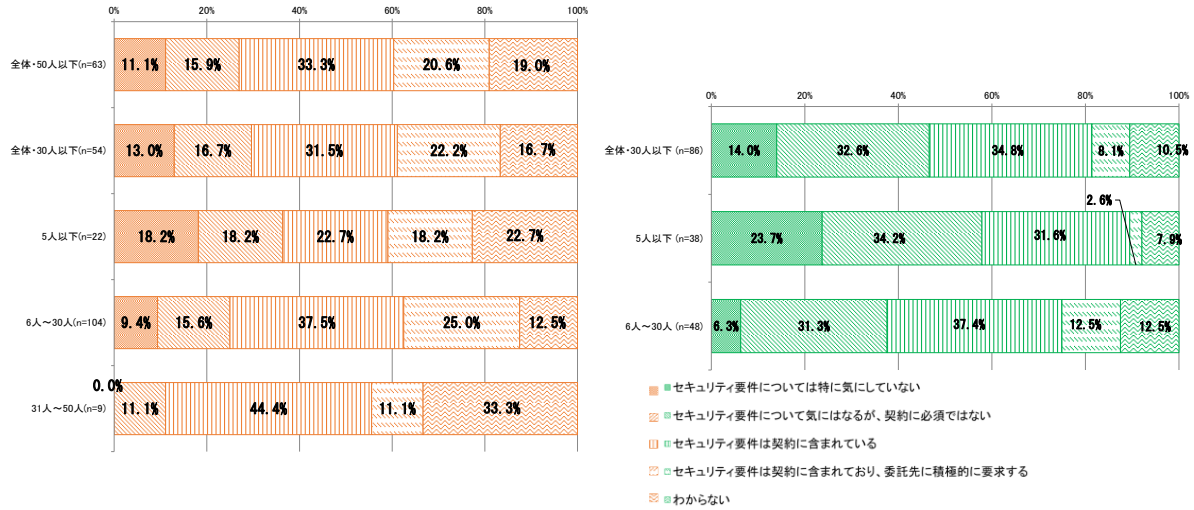

図 2.4.21 セキュリティ要件（本調査 問 10）

2012 年度調査と比較すると、契約に必須ではないという回答が低下している傾向がある。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%、2012 年度調査では 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。

2.4.5. ウェブサイトの重要性・コストの変化について

(1)ウェブサイトの重要性・事業影響度の変化

ウェブサイトの重要性・事業影響度の変化を質問した。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（12.6%）」「高まった（29.9%）」という回答の合計は 42.5%と多い傾向にある。また、従業員別では、6 人～30 人の組織では 50.0%が「大幅に高ま

った（12.5%）」、「高まった(37.5%)」という回答であり、5 人以下の組織の 34.3%よりも多く、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。

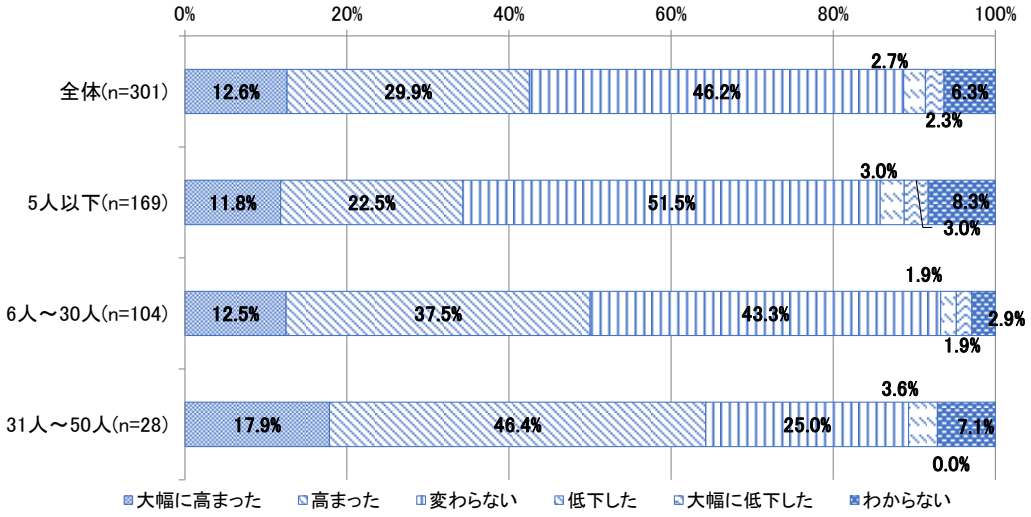

図 2.4.22 ウェブサイトの重要性・事業影響度の変化（本調査 問 6）

(2)ウェブサイトのセキュリティ対策コストの増減

この 10 年程度のウェブサイトのセキュリティ対策コストの増減を質問した。全体では、「変わらない」が 63.8%と最も高く、次いで「大幅に増加した」、「増加した」の合計 19.6%である。また、従業員別では、6 人～30 人の組織では 23.0%が「大幅に増加した」、「増加した」という回答であり、5 人以下の組織の 16.0%よりも多く、従業員数が多いほどウェブサイトのセキュリティ対策コストが増加している傾向がある。

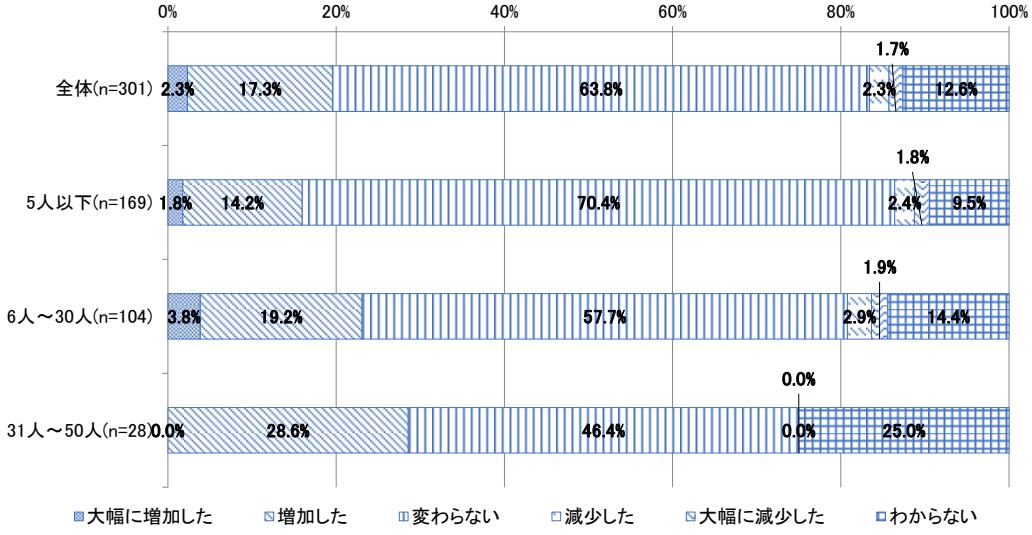

図 2.4.23 ウェブサイトのセキュリティ対策コストの増減（本調査 問 14）

(3)ウェブサイト構築コストの変化

この 10 年程度のウェブサイトの構築コストの増減を質問した。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。また、従業員別では、6 人～30 人の組織では 28.9%が「大幅に増加した」、「増加した」という回答であり、5 人以下の組織の 19.6%よりも多く、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。

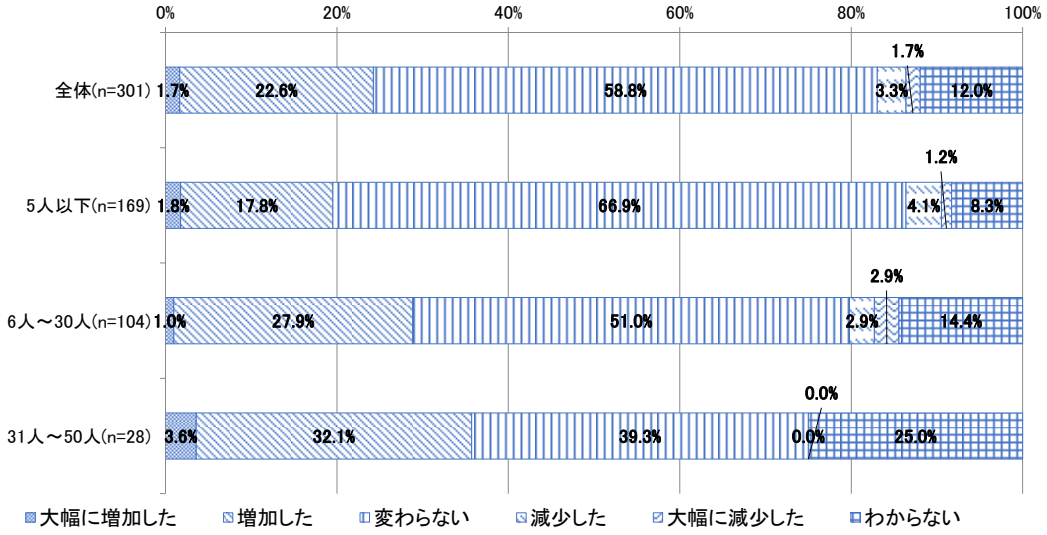

図 2.4.24 ウェブサイト構築コストの増減（本調査 問 16）

(4)ウェブサイトの運用コストの増減

この 10 年程度のウェブサイトの運用コストの増減を質問した。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。また、従業員別では、6 人～30 人の組織では 27.8%が「大幅に増加した」、「増加した」という回答であり、5 人以下の組織の 15.4%よりも多く、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。

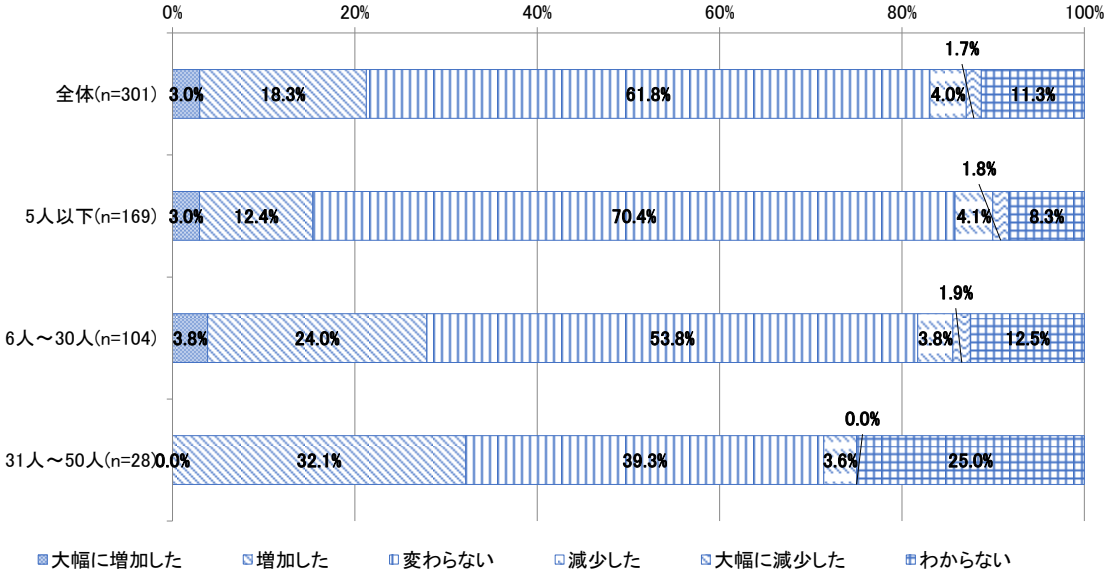

図 2.4.25 ウェブサイトの運用コストの増減（本調査 問 18）

2.4.6. ウェブサイトの脆弱性対策の状況について

(1) ウェブサイトの脆弱性の認識

ウェブサイトの脆弱性対策について解説を示した上で、どの程度知っていたかを質問した。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」という回答が得られた。

2012 年度調査では、約 50%が「詳しく知っている」と回答し、約 30%が「聞いたことがある」という回答であり、脆弱性を「詳しく知っている」という回答は 2012 年度調査に比べ低下している。

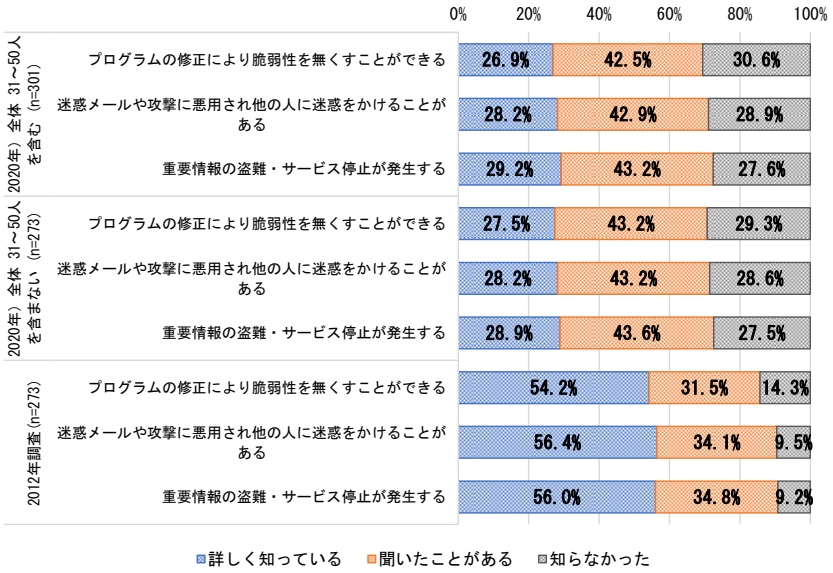

図 2.4.26 ウェブサイト脆弱性の認知度（本調査 問 11-1）

脆弱性に関する具体的な内容については、「SQL インジェクション」や「OS コマンド・インジェクション」等については、約 50%から 60%が知らないという回答であった。

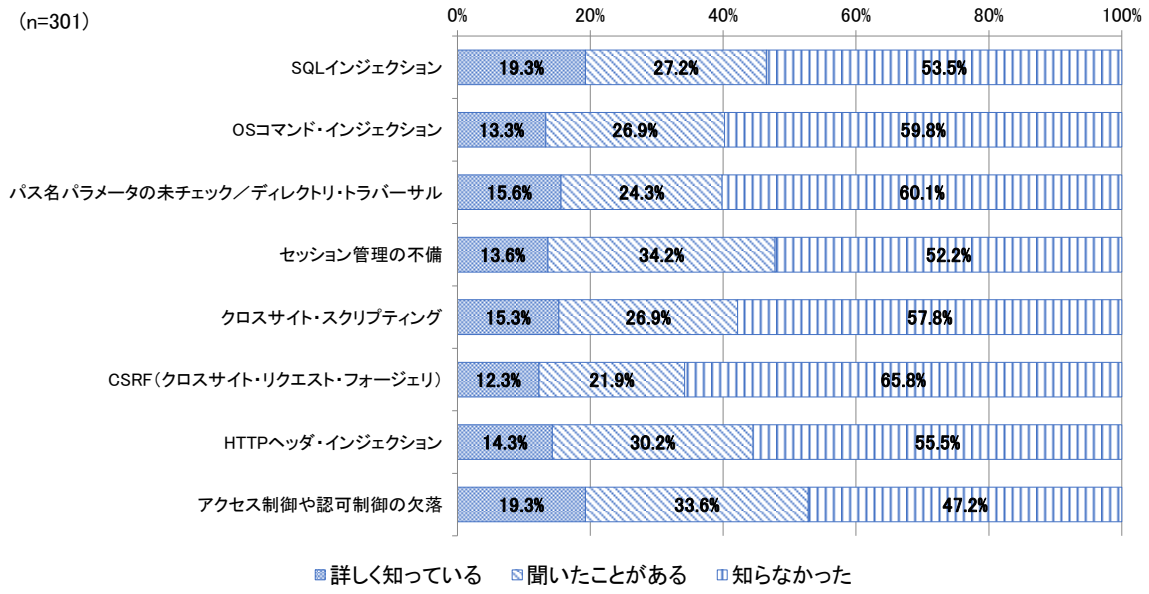

図 2.4.27 ウェブサイト脆弱性の認知度（本調査 問 11-2）

(2) ウェブサイトに対する基本的な脆弱性対策の状況

ウェブサイトに対する基本的な脆弱性対策の状況について質問した（複数回答可）。実施したことがない対策は、「脆弱性（脅威、手口など）の最新情報取得」が 50.2%、「定期的な設定の見直し」が 46.2%であり、「ソフトウェアの定期的な更新」、「セキュリティ製品利用」、「パスワードの管理・認証の強化」は 30%以上が実施していない。

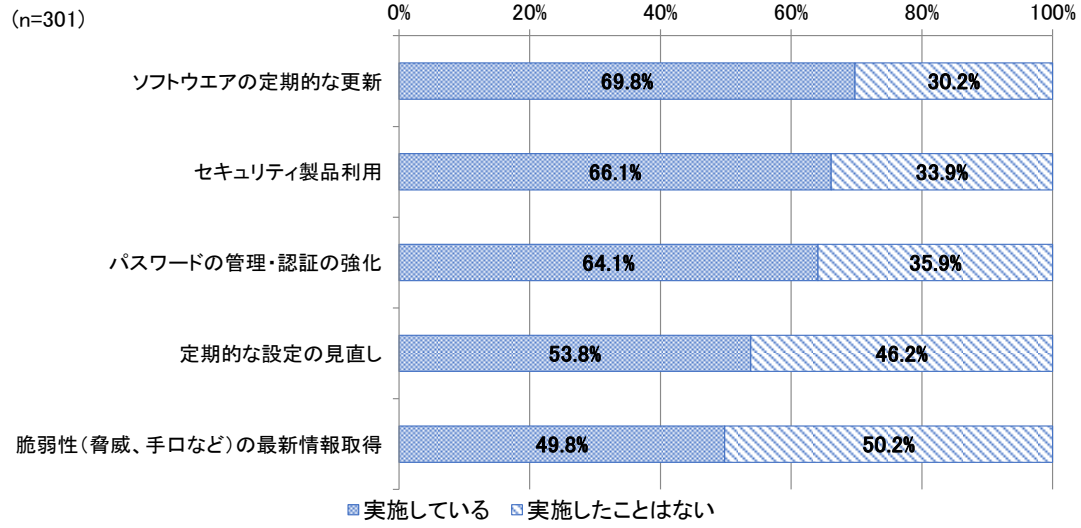

図 2.4.28 ウェブサイトに対する基本的な脆弱性対策の状況（本調査 問 13）

(3)ウェブサイト運用時の脆弱性対策の状況

ウェブサイトの運用時の脆弱性対策の状況について質問した（複数回答可）。実施したことがない対策は、「利用しているネットワーク機器の脆弱性対策」が 47.8%と最も多く、次いで「ウェブサーバの OS の脆弱性対策」が 45.8%、「不正な通信の遮断や通信のフィルタリング」が 44.5%であった。また、その他の対策においても約 40%程度が実施したことがないという回答であった。

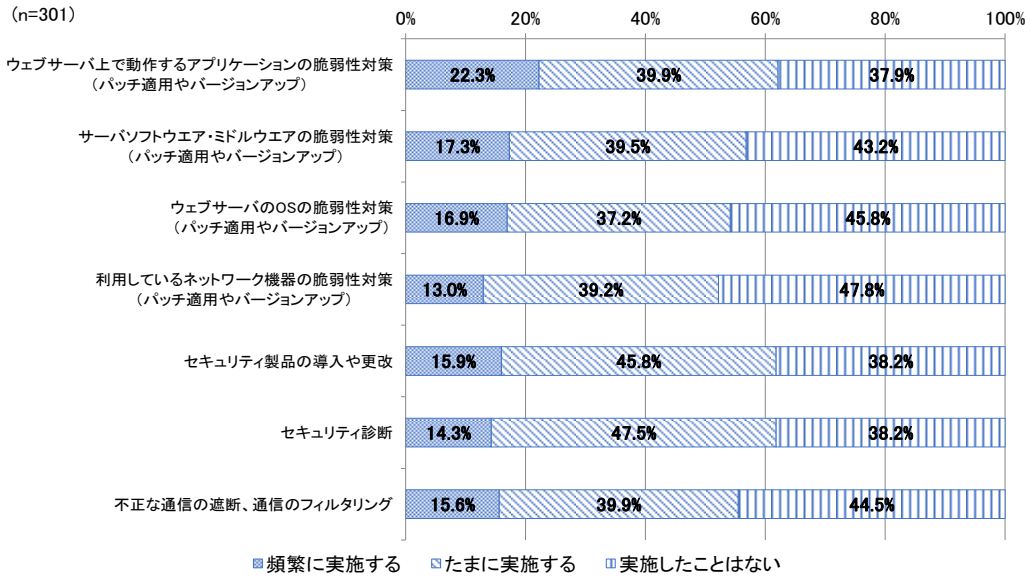

図 2.4.29 ウェブサイト運用時の脆弱性対策の状況（本調査 問 15）

また、同項目 7 つの対策について、全項目を対策していないが 24.9%、1 つの対策を実施しているのは 4.3%、2 対策は 5.3%、3 対策は 7.0%、4 対策は 7.3%、5 対策は 6.6%、6 対策は 5.6%であり、全項目を実施しているのは 38.9%であった。

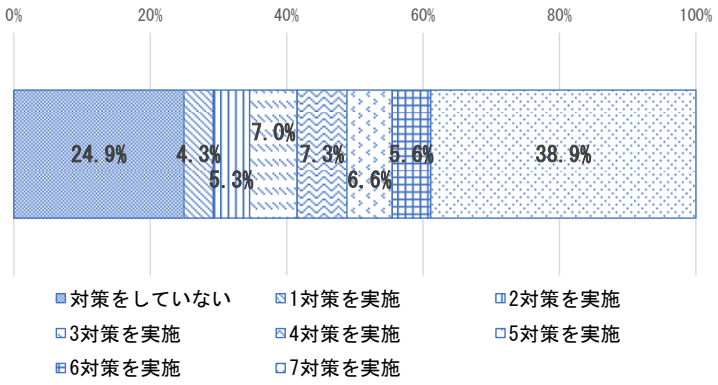

図 2.4.30 ウェブサイト運用時の複数の脆弱性対策の状況（本調査 問 15・複数対策）

ウェブサイトの構築年数ごとの運用時対策状況を示す。5 年未満（図 2.4.31）、5 年以上～10 年未満（図 2.4.32）、10 年以上（図 2.4.33）で運用時の対策状況に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。

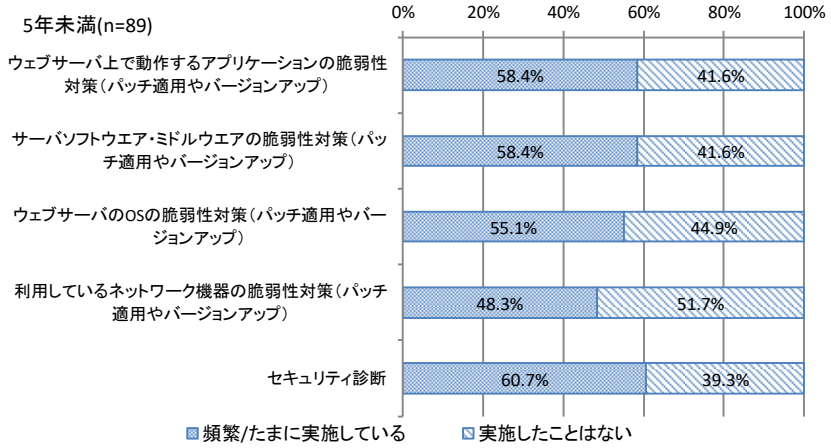

図 2.4.31 ウェブサイトの構築後の年数と基本的な脆弱性対策の実施状況（問 7(5 年未満)と問 15）

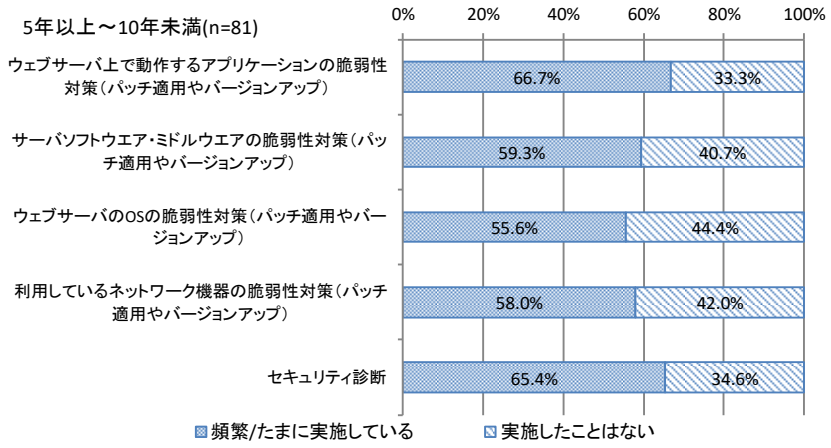

図 2.4.32 ウェブサイトの構築後の年数と基本的な脆弱性対策の実施状況（問 7(5 年以上～10 年未満)と問 15）

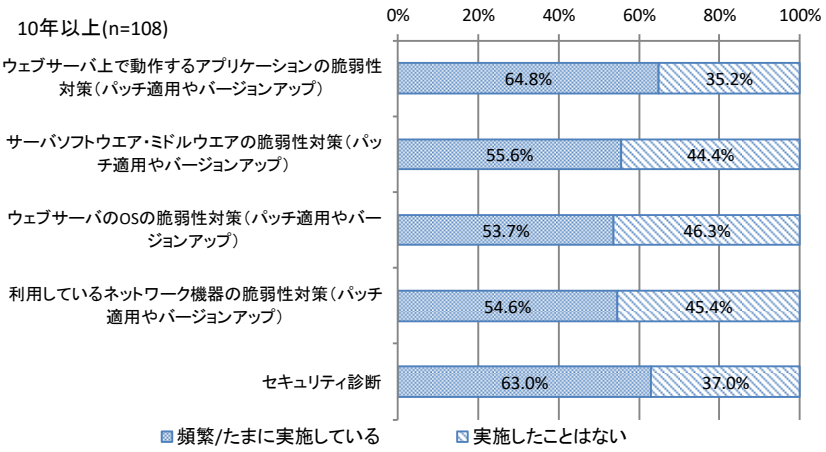

図 2.4.33 ウェブサイトの構築後の年数と基本的な脆弱性対策の実施状況
（問 7(10 年以上)と問 15）

(4) 脆弱性対策の実施状況

(a) 構築時の脆弱性対策

ウェブサイトを構築する際に実施している脆弱性対策について質問した（複数回答可）。「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。2012 年度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。

また、「構築の時点では脆弱性対策をしていない」という回答は全体の 23.9%であった。2012 年度調査では、「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。

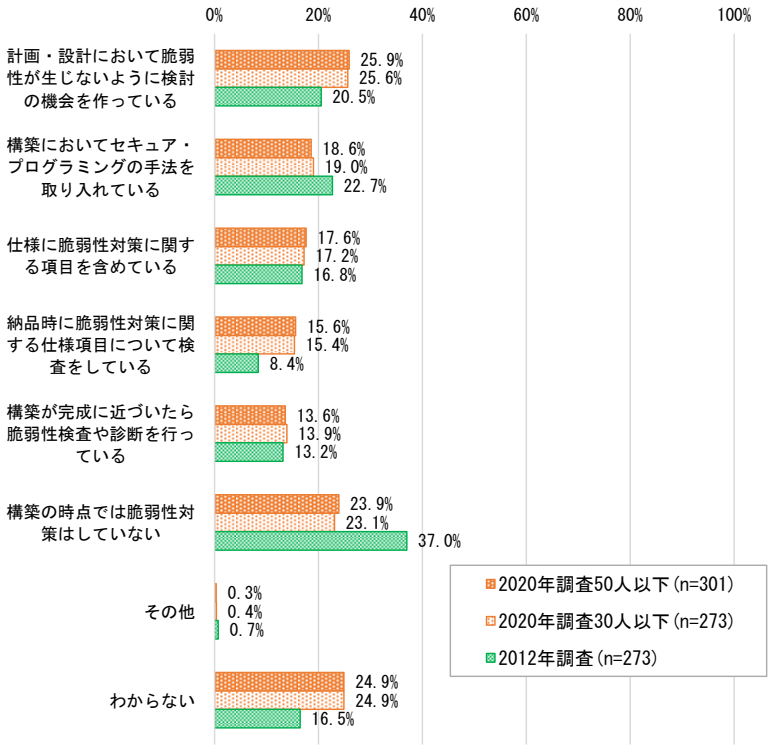

図 2.4.34 構築時の脆弱性対策の内容（本調査 問 17）

(b) 運用時の脆弱性対策

ウェブサイトを運用する際に実施している脆弱性対策について質問した（複数回答可）。「脆弱性が発見されたら、可能な限り速やかに修正を行っている」が 40.9%と最も多く、次いで「脆弱性が発見されたら、その深刻さについて調べ、対処方法を検討する」が 20.9%であった。2012 年度調査においても同様の傾向がある。

また、運用において脆弱性対策をしていないという回答は全体の 13.3%であり、2012 年度調査においても 17.2%であった。

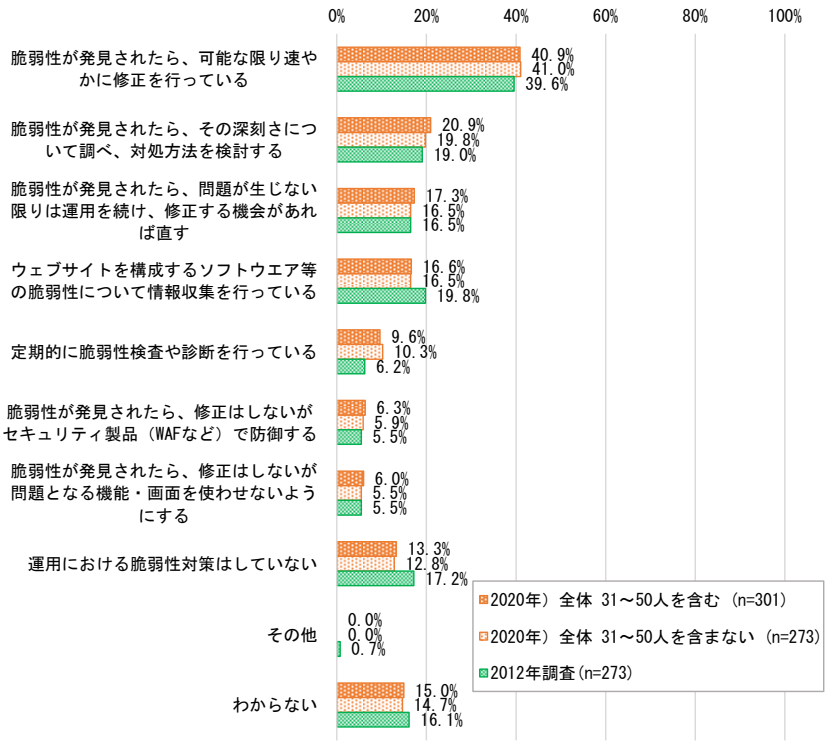

図 2.4.35 運用時の脆弱性対策の内容（本調査 問 19）

(c) 脆弱性対策の実施状況

ウェブサイトの構築時および運用時に何らかの脆弱性対策を行っているかどうかを集計した（いずれかの設問で構築時や運用時に対策しているとした回答は各々の「対策している」に集約している）。「構築時も運用時も脆弱性対策をしている」とした回答者は 48.8%であり、「運用時にのみ脆弱性対策している」とした回答は 22.9%であった。「一切脆弱性対策をしていない」とした回答者は全体の 9.6%であった。2012 年度調査でも同様の傾向があり、「構築時も運用時も脆弱性対策をしている」とした回答者は 45.4%、「運用時にのみ脆弱性対策している」とした回答は 21.2%、「一切脆弱性対策をしていない」とした回答者は 16.8%であり、「構築時にのみ脆弱性対策をしている」という回答は少ない。

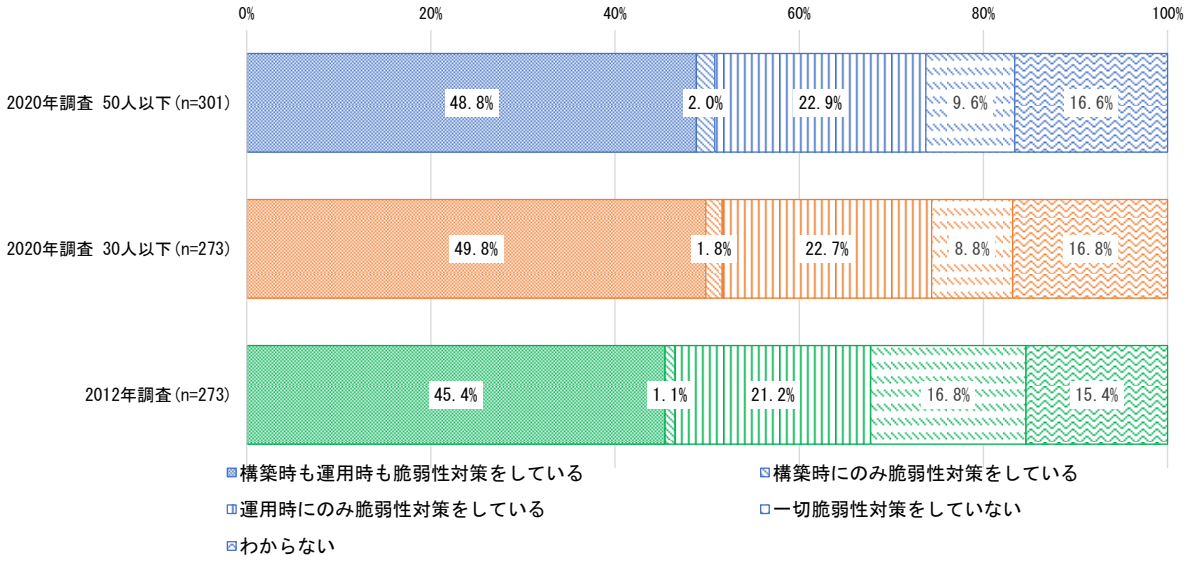

図 2.4.36 脆弱性対策の実施状況（本調査 問 17 および問 19）

(d) 脆弱性対策を行わない理由

構築時あるいは運用時にウェブサイトの脆弱性対策を行わないとした回答者にその理由を質問した（複数回答可）。「個人情報を扱っていないから」(51.8%)、「クレジットカード等の決済を行っていないから」(38.6%)、「サイトが著名でないので、被害に遭うとは考えにくいから」(27.7%)とする回答が上位を占めた。2012 年度調査においても同様の傾向があり、「クレジットカード等の決済を行っていないから」(59.8%)、「個人情報を扱っていないから」(58.8%)、「サイトが著名でないので、被害に遭うとは考えにくいから」(33.3%)とする回答が上位を占めている。一方で、本年度調査の回答は、2012 年度調査の回答と比べ、「クレジットカード等の決済を行っていないから」が低く、「難しくてよくわからない」が高い。

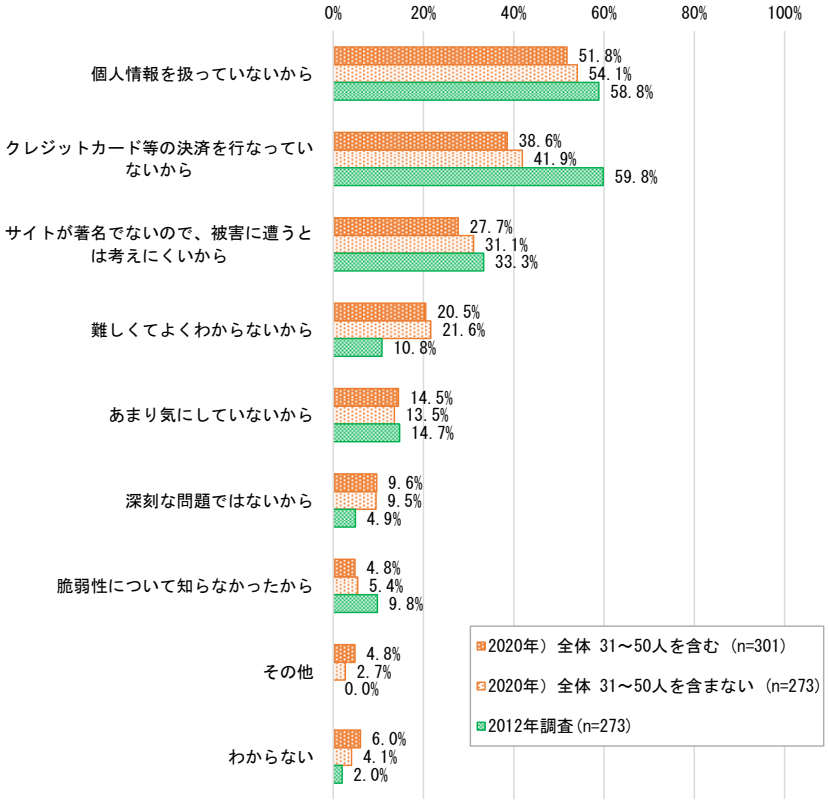

図 2.4.37 脆弱性対策を行わない理由（本調査 問 20）

(5) 脆弱性に気付いたきっかけ

ウェブサイトの脆弱性に気付いたきっかけについて質問した（複数回答可）。「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て示した回答は合わせて 31.3%であった。2012 年度調査では、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 17.2%であり、組織外からの連絡を受けることが多くなっている傾向がある。また、「脆弱性がみつかったことはない」とする回答は全体の 33.9%であり、2012 年度調査の 54.2%よりも低い。

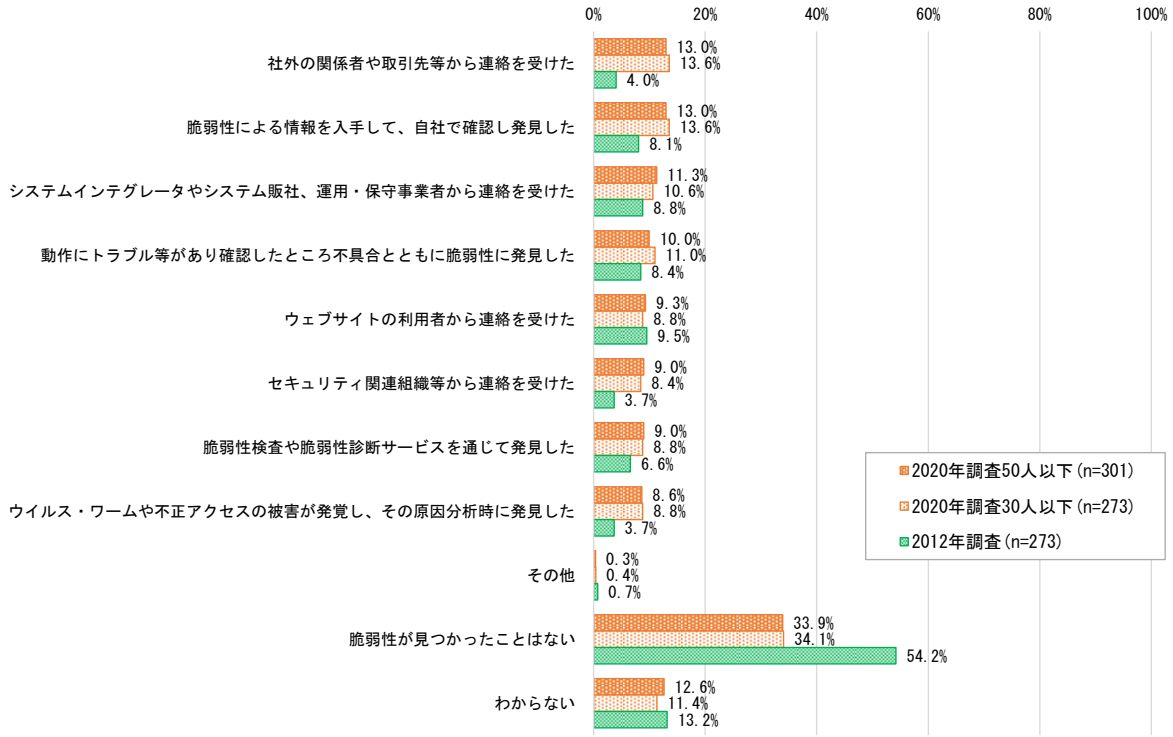

図 2.4.38 脆弱性に気付いたきっかけ（本調査 問 21）

(6) 脆弱性に起因する被害の経験

ウェブサイトの脆弱性対策の遅れやミスが間接的な原因となって、改ざん、不正アクセス、サーバのダウン等の被害に遭った経験があるかを質問した。被害に遭ったことがあるという回答は合わせて全体の 20.3%（業務に影響が生じる被害が発生したことがある 5.0%、被害に遭ったことはあるが実害が発生したことはない 15.3%）であった。従業員規模別では、被害に遭ったことがあるという回答は、5 人以下の組織は 17.7%、6 人～30 人の組織は 23.1%、31 人～50 人の組織は 25.0%であり、従業員規模が大きいほど被害に遭っている傾向がある。

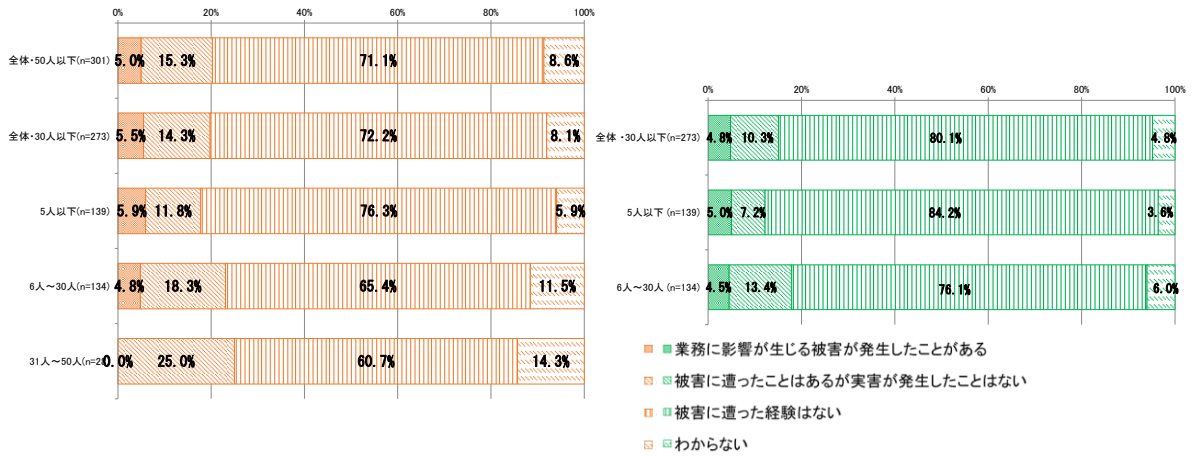

図 2.4.39 脆弱性に起因する被害の経験（本調査 問 23）

2012 年度調査に比べ、被害に遭ったことがあるという回答は、本年度調査では 19.8%、2012 年度調査では 15.1%であり、被害の経験があるという回答が微増している。

「業務に影響が生じる被害が発生したことがある」、「被害に遭ったことはあるが実害が発生したことはない」という回答と脆弱性発見時の対処をクロス集計した結果を以下に示す。全体として「脆弱性が発見されたら、可能な限り速やかに修正を行っている」が 47.5%であり、同項目について、業務に影響が生じた被害の回答は 40.0%、実害が発生しなかった被害の経験の回答は 50.0%であった。

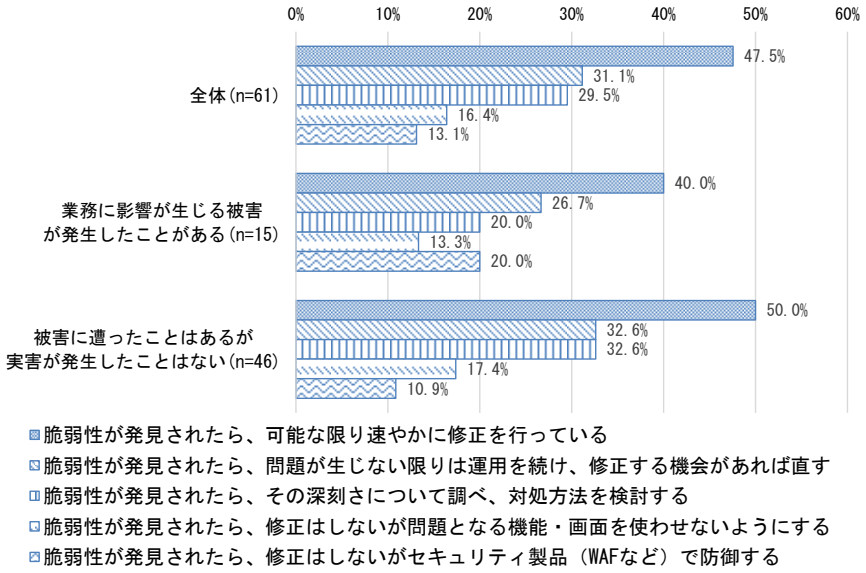

図 2.4.40 被害経験と脆弱発見時の対処（本調査 問 19 と問 23）

(7) セキュリティ対策（脆弱性対策）の費用・人員の確保

ウェブサイトの脆弱性対策・セキュリティ対策に必要な費用や人員がどの程度確保されているかを質問した。「十分に確保できている」、「おおむね確保できている」という回答を合わせ全体で 40.9%、「やや不足している」、「全く足りていない」という回答を合わせ全体で 37.6%であった。従業員規模別においても同様の傾向があり、「十分に確保できている」、「おおむね確保できている」という回答は、5 人以下の組織は 42.6%、6 人～30 人の組織は 37.5%、31 人～50 人の組織は 42.9%である。2012 年度調査も同じ傾向である。

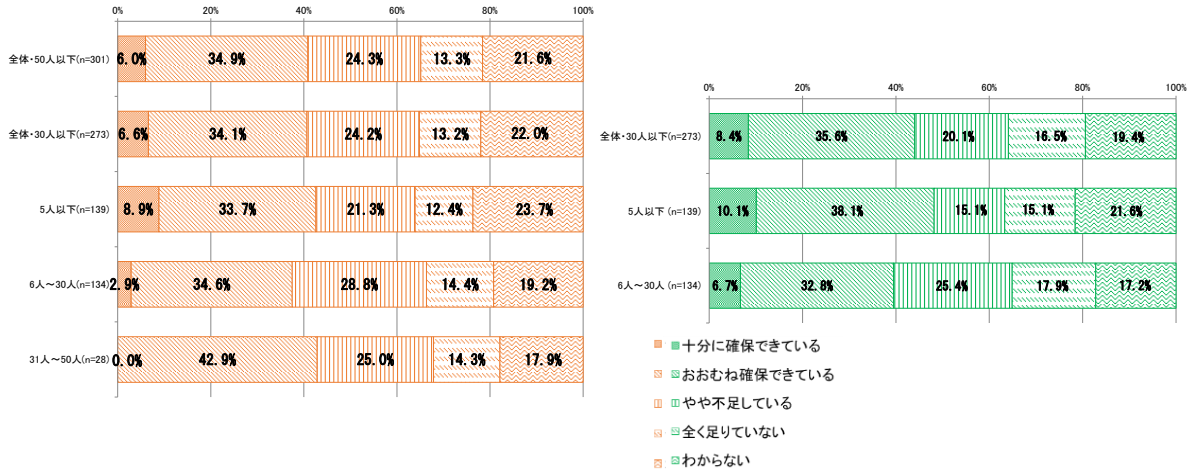

図 2.4.41 セキュリティ対策（脆弱性対策）の費用・人員の確保（本調査 問 25）

(8) セキュリティ対策（脆弱性対策）に関する判断を行う人

ウェブサイトの脆弱性対策などのセキュリティ対策について、対策を適用すべきか否か等を判断する人は誰かを質問した。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。従業員規模別では、5 人以下の組織は、「組織のトップ」が 46.7%と最も多く、次いで「特に決まっていない」が 23.1%であり、他に比べ組織のトップが著しく多い。6 人～30 人の組織は、「ウェブサイト管理の責任者」が 31.7%と最も多く、次いで「組織のトップ」が 26.9%であった。31 人～50 人の組織は、「ウェブサイト管理の責任者」が 39.3%と最も多く、次いで「特に決まっていない」が 32.1%であり、他に比べ特に決まっていないが多い。

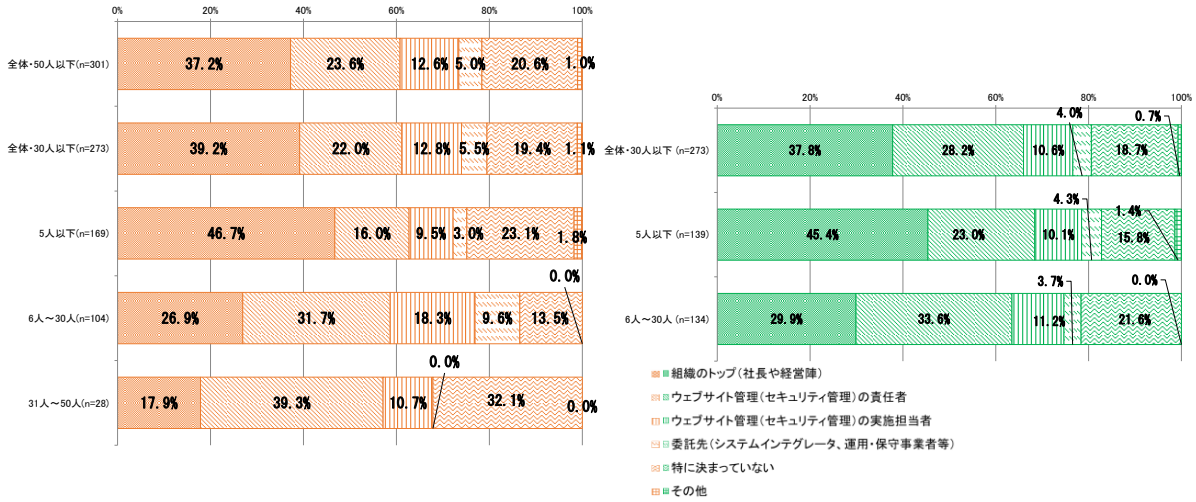

図 2.4.42 セキュリティ対策（脆弱性対策）に関する判断を行う人（本調査 問 22）

2012 年度調査と比較すると、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。従業員規模別では、本年度調査の 5 人以下の

組織は、回答の多い順に「組織のトップ」(46.7%)、次いで「特に決まっていない」(23.1%)、「ウェブサイト管理の責任者」(16.0%)であるが、2012 年度調査の 5 人以下の組織は、回答の多い順に「組織のトップ」(45.4%)、次いで「ウェブサイト管理の責任者」(23.0%)、「特に決まっていない」(15.8%)であった。本年度調査の 6 人～30 人の組織は、回答の多い順に「ウェブサイト管理の責任者」(31.7%)、次いで「組織のトップ」(26.9%)、「ウェブサイト管理の実施担当者」(18.3%)であるが、2012 年度調査の 6 人～30 人の組織は、回答の多い順に「ウェブサイト管理の責任者」(33.6%)、次いで「組織のトップ」(29.9%)、「特に決まっていない」(21.6%)であった。

(9) 脆弱性対策を実際に行う人

運用中のウェブサイトに脆弱性が発見された場合に、サイトの一時停止、該当箇所の修正、回避策の適用等の作業を誰が行うかを質問した。全体では、「ウェブサイト管理の実施担当者」(47.2%)が最も多く、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」(16.9%)、次に「特に脆弱性対策は取らない」(13.6%)であった。

従業員規模別では、5 人以下の組織と 31 人～50 人の組織は他に比べて、「ウェブサイト管理の実施担当者」が多く、6 人～30 人の組織は他に比べて「委託先のシステムインテグレータや運用・保守事業者」が多い傾向である。

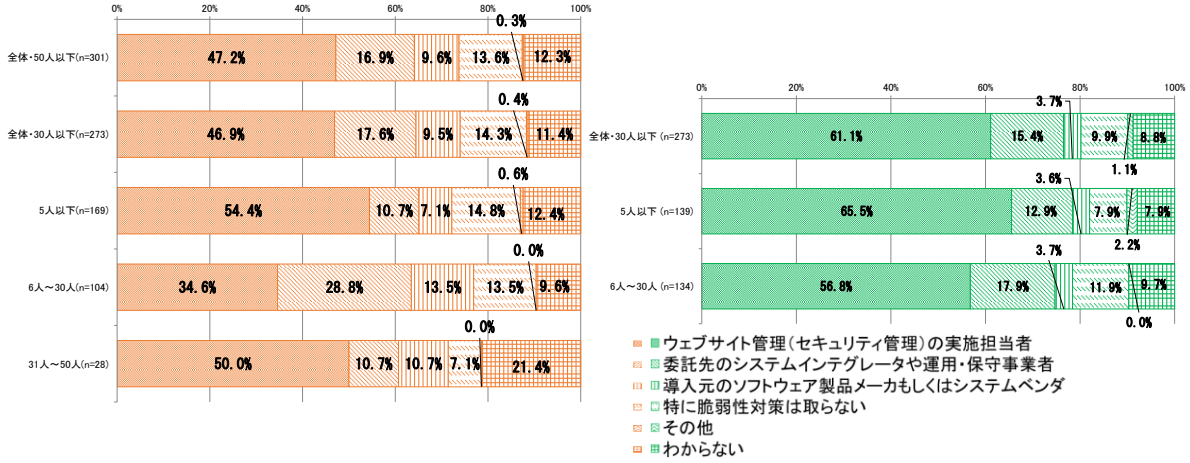

図 2.4.43 脆弱性対策を実際に行う人（本調査 問 24）

本年度調査と 2012 年度調査の傾向は全体では同じであり、回答の多い順に「ウェブサイト管理の実施担当者」、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」、「特に脆弱性対策は取らない」であるが、「ウェブサイト管理の実施担当者」は、本年度調査では 46.9%、2012 年度調査では 61.1%であり、本年度調査の回答は 2012 年度調査に比べ低く、自組織での対応が低くなっている傾向がある。

(10) セキュリティ対策（脆弱性対策）の課題

ウェブサイトの脆弱性対策等のセキュリティ対策を進める上での課題について質問した。「重要

な課題」、「課題のひとつ」を合わせた回答が多い順番で「(2)脆弱性やセキュリティに関する技術の習得が難しい」(74.4%)、「(5)脆弱性やセキュリティに関する情報が多すぎて選別が難しい」(64.2%)、「(3)対策を行うための人員が足りない」(63.5%) を挙げる回答が多かった。

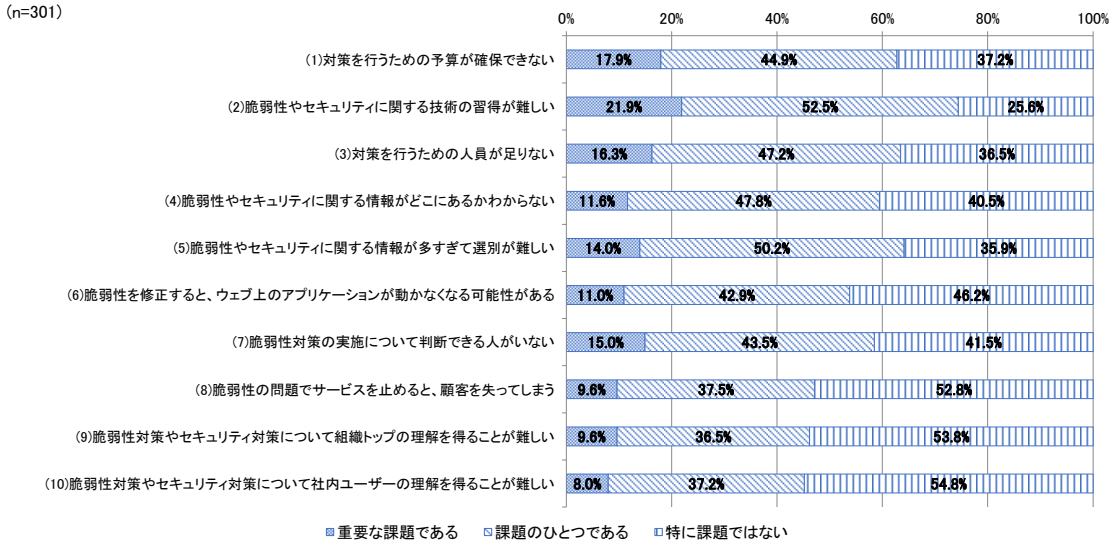

図 2.4.44 セキュリティ対策（脆弱性対策）の課題（本調査 問 26）

2012 年度調査では、重要な課題及び課題のひとつを合わせた回答が多い順番で「(2)脆弱性やセキュリティに関する技術の習得が難しい」、「(5)脆弱性やセキュリティに関する情報が多すぎて選別が難しい」、「(1)対策を行うための予算が確保できない」続いて「(3)対策を行うための人員が足りない」が多く、同様の傾向であった。

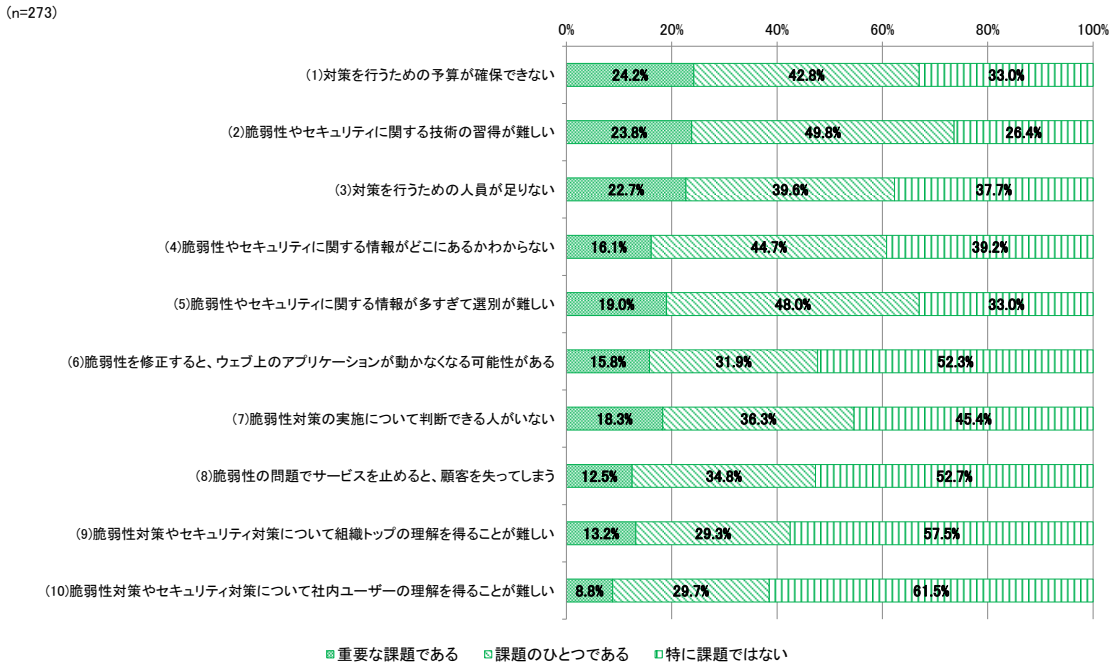

図 2.4.45 セキュリティ対策（脆弱性対策）の課題 2012 年度調査結果

(11)脆弱性の被害事例の知った時の行動

国内のウェブサイトへの脆弱性を悪用した攻撃などによって企業や組織が被害を受けていることを知った時にどうするかを質問した。全体では、「被害事例を参考に、対策をしたいが、十分に対応できていない」(46.2%)が最も多く、次いで「被害事例は気になるが、何もしない」(24.9%)、「被害事例を参考に、自社のウェブサイトのセキュリティ対策を確認、見直し等をしている」(23.6%)であり、被害事例を参考に見直しをしない(対応できない、何もしない、気にならない)は、約 70%であった。この傾向は従業員規模別でも同様であり、被害事例を参考に見直しをしないは、約 70%であるが、31 人～50 人の組織は、「被害事例を参考に、対策をしたいが、十分に対応できていない」(57.1%)が他に比べて多い。

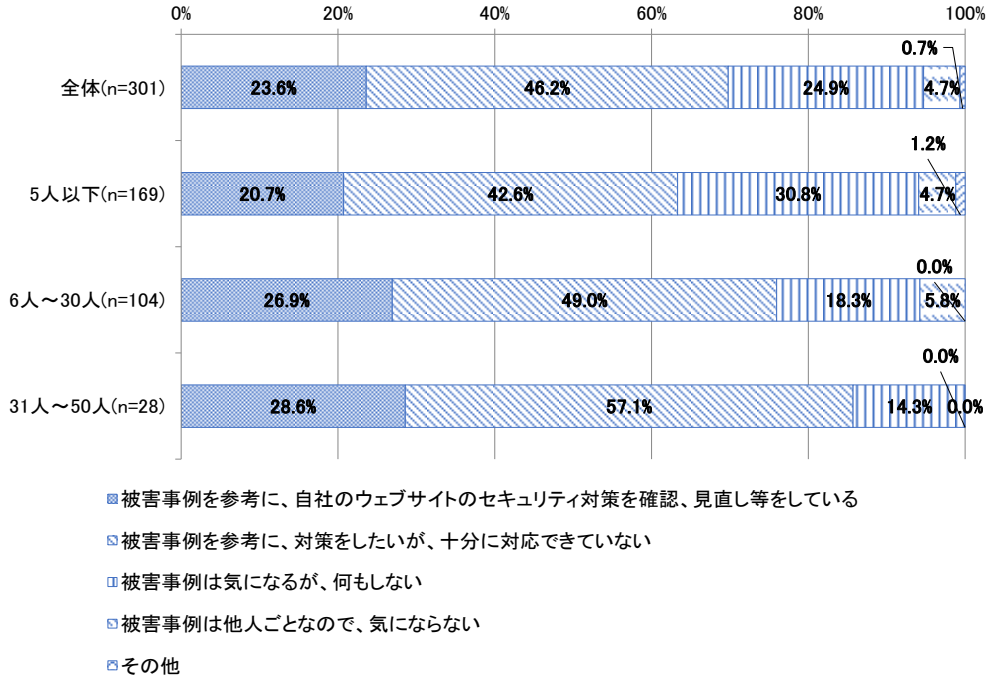

図 2.4.46 脆弱性の被害事例の知った時の行動（本調査 問 12）

2.4.7. セキュリティ対策（脆弱性対策）に関する取組みについて

(1) 情報セキュリティ早期警戒パートナーシップの認知状況

情報セキュリティ早期警戒パートナーシップについて解説を示した上で、これまでに知っていたかを質問した。聞いたことがあるとする回答は合わせて約 50%であり、2012 年度調査の約 40%に比べ多い。

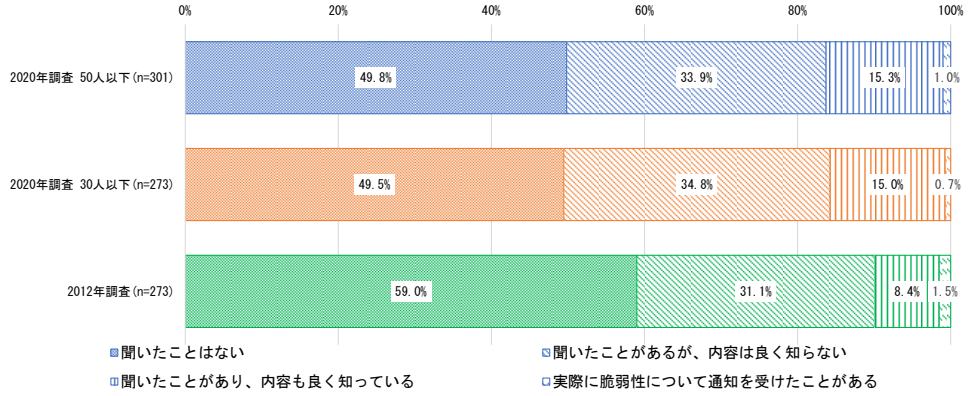

図 2.4.47 情報セキュリティ早期警戒パートナーシップの認知状況（本調査 問 27）

(2) IPA による脆弱性関連の情報等の認知状況

IPA より提供されている脆弱性対策・セキュリティ対策に関する情報について、リンクの URL と共に、これまでに知っていたかを質問した。少なくとも聞いたことがあるとする回答を合わせると、最も知られているものは「安全なウェブサイトの作り方」（全体の 40.9%）であった。また、聞いたことがないとする回答は、すべての情報において約 60%から 70%であった。

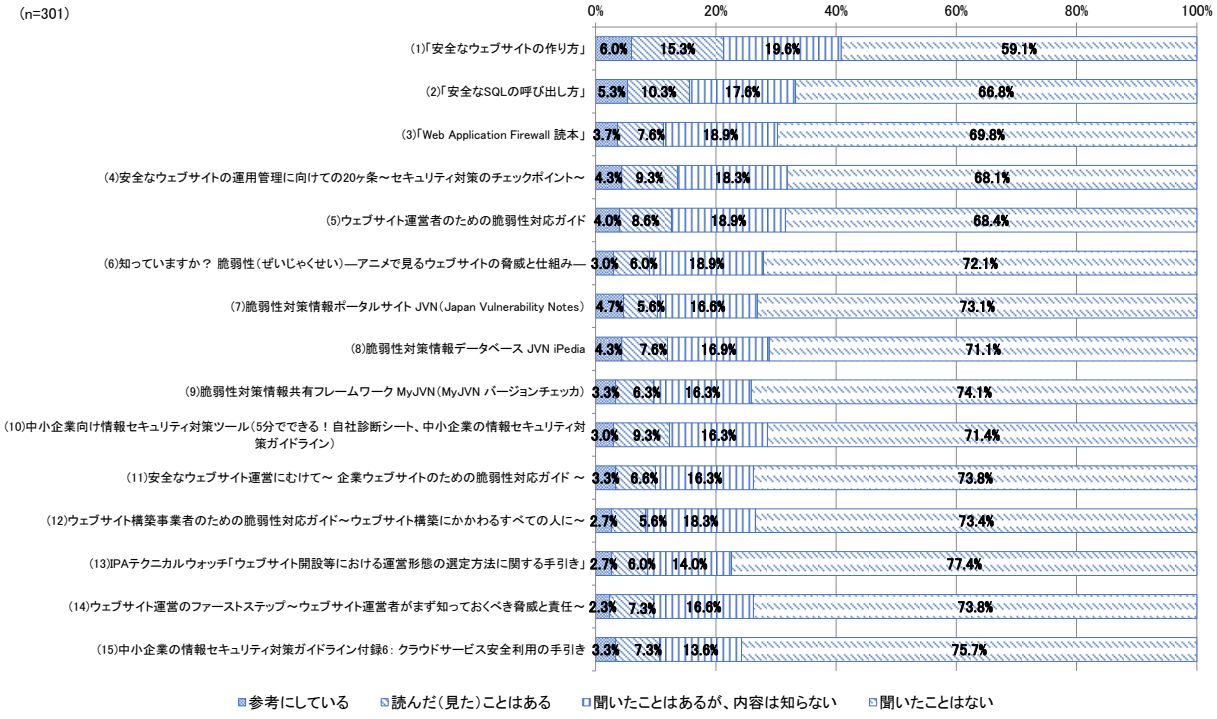

図 2.4.48 IPA による脆弱性関連の情報等の認知状況（本調査 問 28）

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」（全体の 36.2%）であった。また、聞いたことがないとする回答は、すべての情報において約 60%から 80%であった。

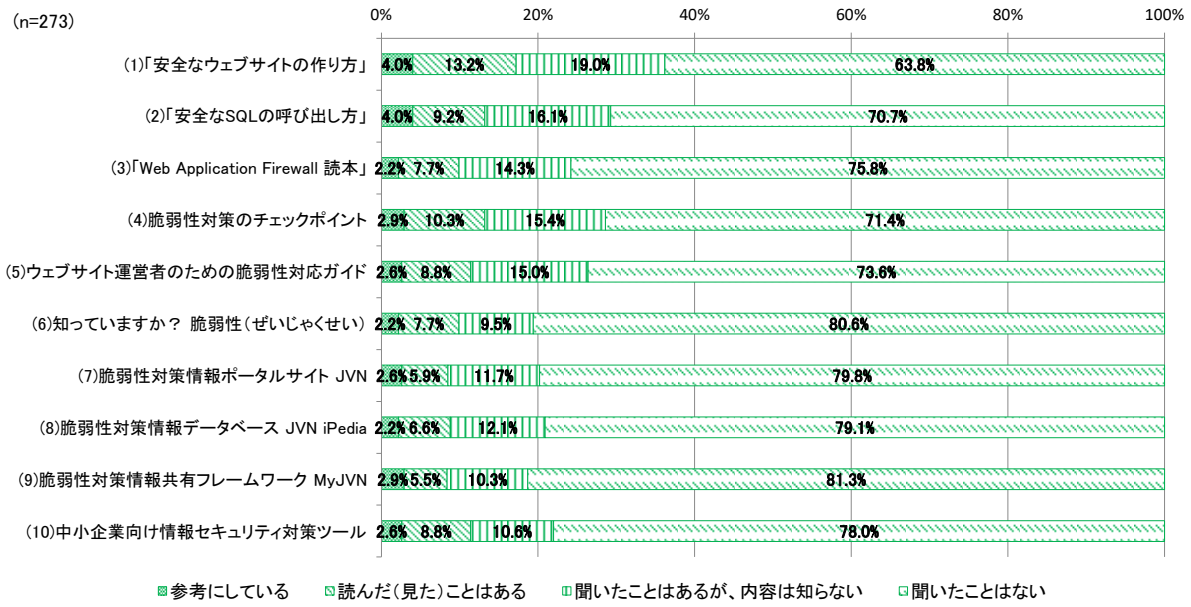

図 2.4.49 IPA による脆弱性関連の情報等の認知状況 2012 年度調査結果

(3) 利用してみたい普及・啓発コンテンツ

情報セキュリティに関してどのような普及啓発コンテンツを利用してみたいかを確認した（複数選択可）。「ウェブサイトのセキュリティ対策の運用・管理に関するコンテンツ」(37.2%)、「セキュアなウェブサイトの構築に関するコンテンツ」(31.9%)、「最近のウェブサイトに関するセキュリティ脅威の動向が分かるコンテンツ」(30.9%)について比較的高い関心が示された。この傾向は、2012 年度調査においても同様である。

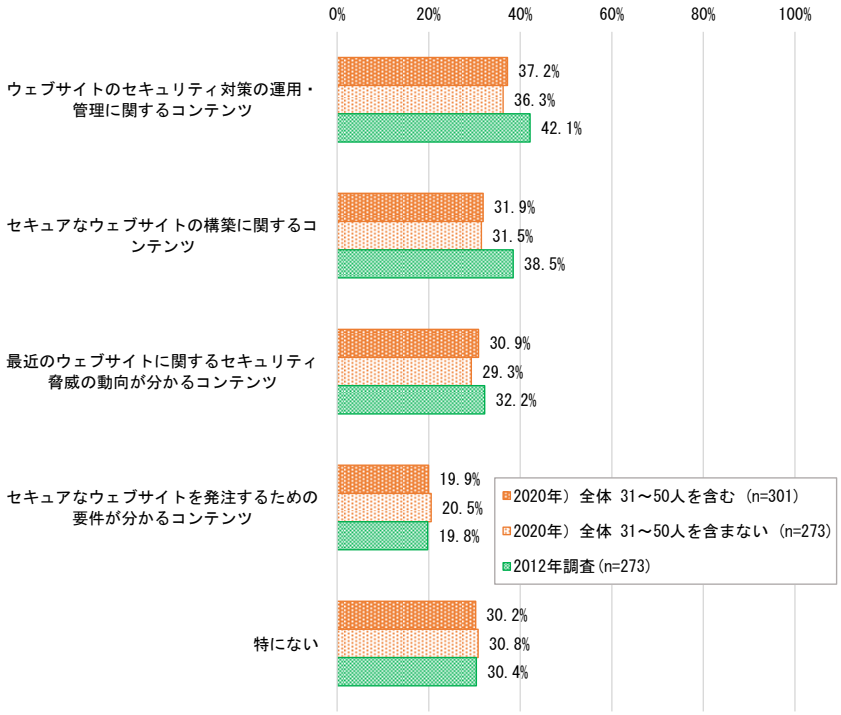

図 2.4.50 利用してみたい普及・啓発コンテンツ（本調査 問 29）

2.5. 考察

2.5.1.調査対象者について

本調査は、ウェブモニターを対象としたアンケート調査であるため、調査に回答できる程度以上の IT・インターネット技術に関する知見を持つ者を対象としている。また、予備調査でウェブサイトに関連しうる業務に従事している者を抽出し、それらを対象に本調査を行っている。

調査結果については、小企業においても特に IT やインターネット技術に関して高いリテラシーを持つ者から得た回答に基づいている。また、業種としては「情報通信、IT 関連サービス」に属する回答者の比率が高い。加えて、自身の主担当業務を経営と考えて回答した経営者は本調査の対象から外れている点についても注意が必要である。

2.5.2.仮説の検証

(1) ウェブサイトの構築・運用の実態について

(仮説 1) 自社社員が少人数（ほぼ 1 名）で運用者が不明確

ウェブサイトにトラブルが生じたときに「自身がトラブルに対処する」と答えた回答者は全体の 44.5%であった。(予備調査 問 9)

また、ウェブサイトのセキュリティ管理を「組織的には行っていない」小企業は 39.1%であった。他方で「担当者がいる」小企業は 32.7%、「主担当業務以外にウェブサイトのセキュリティ管理を兼任する担当者がいる」小企業は 15.7%となり、担当者がいると答えた回答を合計すると 48.4% となった。(本調査 問 9)

これらの結果から、半数程度で担当者が定まっており、仮説は必ずしも正しいとは言えないが、少人数でウェブサイトの運用をしている様子が伺われる。

なお、ウェブサイトの脆弱性対策・セキュリティ対策に必要な費用や人員については、充分に確保できているが 6.0%、おおむね確保できているが 34.9%と確保できている率は合計 40.9%、やや不足しているが 24.3%、全く足りてないが 13.3%と確保できていない率は合計 37.6%という結果であった。(本調査 問 25)

(仮説 2) 構築および運用の方針は経営者が決定

ウェブサイトの運用・構築についてのトップ（社長や経営陣）の関与の状況は、「トップ自らが運用・構築にあたっている」小企業が 35.5%であった。この割合は従業員数 5 人以下の企業では 56.8%であったが、6 人～30 人の企業では、8.7%だった。また、「積極的に担当者に指示を出す」小企業は、全体で 20.3%であり、5 人以下の企業では 14.2%、6 人～30 人の企業では、29.8%であった。(本調査 問 5)

脆弱性対策等のセキュリティ対策の適用について「組織のトップ」が判断する小企業は 37.2%であった。(本調査 問 22)

これらの結果から、仮説は必ずしも正しいとは言えないが、より小規模な組織ほど、経営層が

関わっている様子が伺える。

(仮説 3) セキュリティ対策は運用段階の対策を実施している

脆弱性対策の実施状況については、「構築時も運用時も脆弱性対策をしている」小企業が全体の 48.8%と最も多く、次いで「運用時にのみ対策をしている」小企業が 22.9%であった。「構築時にのみ対策をしている」小企業は皆無に近い状態（2.0%）であった。(本調査 問 17 および本調査 問 19)

これらの結果から、運用時に対策が行われている様子が伺えた。また、「一切対策をしていない」小企業も 16.6%と多くあった。

(2) 脆弱性対策への理解について

(仮説 4) 脅威を認識しておらず危機感がない（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）

(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

ウェブサイトの機能・画面について、脆弱性対策が必要となる例を挙げて質問したところ、半数以上の小企業のウェブサイトには脆弱性対策が必要と考えられる機能・画面が備えられていた。(予備調査 問 10)

ウェブサイトの脆弱性について知っているか尋ねたところ、約 25～30%は詳しく知っており、約 40%は聞いたことがあるという結果を得た。(本調査 問 11)

脆弱性対策を行わないと答えた者にその理由を尋ねたところ、「個人情報を扱っていない」(51.8%)「クレジットカード等の決済を行っていない」(38.6%) という理由が挙げられていた。「サイトが著名でないので、被害に遭うとは考えにくいから」も理由として挙げられているが 27.7%であり、「小企業は攻撃されない」という考え以外の理由もあることが伺われる。(本調査 問 20)

さらに、国内のウェブサイトへの脆弱性を悪用した攻撃などによって企業や組織が被害を受けていることを知った時の行動としては、「被害事例を参考に対策を実施したいが十分にできていない」が 46.2%、「被害事例は気になるが何もしない」が 24.9%で、合計 71.1%という結果であった。(本調査 問 12)

これらから、脆弱性については一定の脅威として認識している場合もあるが、ウェブサイトに積極的に対策を行う強い必要性が認められないため対策を行わないという状況が伺える。

(3) 脆弱性対策の現状と課題について

(仮説 6) ウェブサイトを一時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

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について尋ねたところ、「脆弱性を修正すると、ウェブ上のアプリケーションが動かなくなる可能性がある」、「脆弱性の問題でサービスを止めると、顧客を失ってしまう」のいずれの項目についても、「特に課題ではない」とする回答が 46.2%、52.8%と約半数となった。これらよりも「脆弱性やセキュリティに

関する技術の習得が難しい」(74.4%)や「脆弱性やセキュリティに関する情報が多すぎて選別が難しい」(64.1%)の方が課題と認識されていることが伺われる。(本調査 問 26(6)(8))

このことから、仮説は必ずしも正しいとは言えず、脆弱性の修正に消極的な理由としては、ウェブ上のアプリケーションが動かなくなるやサービスを止めると顧客を失ってしまうことではなく、予算、人材不足、技術習得の難しさが理由として大きい様子が伺える。

(仮説 7) ウェブサイトのセキュリティ対策へ費やす予算や人手が十分ではない

費用と人員の確保状況について、「十分に確保できている」(6.0%)、「おおむね確保できている」(34.9%) とする回答を合わせると約 40%であった。一方、「やや不足している」(24.3%)、「まったく足りていない」(13.3%) とする回答も合わせて 40%近くであった。「わからない」とする回答が 21.6%と多く、適正なコストを見積もれない状況が伺える。(本調査 問 25)

予算と人員の確保について課題とみなす回答は全体の約 60%であった。(本調査 問 26(1)(3))

(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

ウェブサイト担当者の選定理由をたずねたところ、「パソコンに詳しい／慣れているから」とする回答が最も多く (52.5%)、ついで「デザインができるから」、「運営や管理ができるから」といった理由が挙げられた。(本調査 問 8)

「脆弱性やセキュリティに関する技術の習得が難しい」ことを課題として挙げる回答は全体の約 70%であった。(本調査 問 26(2))

これらから、小企業のウェブサイトの運営に関与する経営者や担当者にとって、脆弱性やセキュリティに関する技術が難しく、理解が及んでいない様子が伺えた。

(仮説 9) トラブルが生じても脆弱性対策による根本的な解決は行われない

脆弱性に起因する被害経験について尋ねたところ、「業務に影響が生じる被害が発生した」という回答が全体の 5.0%、「実害が発生したことはないが被害に遭ったことはある」という回答が 15.3%あった。これらを合わせ約 20%の回答者が被害に遭ったと答えている。(本調査 問 23)

運用中のウェブサイトに脆弱性が発見された場合に「特に脆弱性対策は取らない」とする回答は全体の 13.6%であった。(本調査 問 24)

運用中のウェブサイトの脆弱性対策については、運用における脆弱性対策はしていないとする回答は全体の 13.3%であった。(本調査 問 19)

また、脆弱性に起因する被害経験「業務に影響が生じる被害が発生した」、「実害が発生したことはないが被害に遭ったことはある」という回答者について、脆弱性の発見時の対応に関してクロス集計した結果、「可能な限り速やかに修正を行っている」が全体で 47.5%、「脆弱性が発見されたら、その深刻さについて調べ、対処方法を検討する」が全体で 29.5%であった。(本調査 問 19 と問 23)

これらから、仮説は必ずしも正しいとはいえず、脆弱性発見等のトラブルが生じた場合に一定数は修正対応をするといえるが、そうでない場合も一定数あることが伺われる。

(4)IPA の普及啓発資料に関する認知度について

(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

情報セキュリティ早期警戒パートナーシップの取組みについて尋ねたところ、聞いたことがあるとした回答は約 50%であった。(本調査 問 27)

IPA による脆弱性関連の情報等の認知状況については、約 20～40%ほどが聞いたことがあるとしている。(本調査 問 28)

ウェブサイトのセキュリティ対策の運用・管理、セキュアなウェブサイトの構築、最近のウェブサイトに関するセキュリティ脅威の動向などの情報セキュリティに関する普及啓発コンテンツを利用してみたいかを尋ねたところ、何らかのコンテンツを利用してみたいと答えた回答が約 70%であった。

(5)ウェブサイトの対策・重要性の変化

(仮説 11) 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

ウェブサイトでの基本的な脆弱性対策の実施について尋ねたところ、「ソフトウェアの定期的な更新」は 30.2%が実施したことはないという結果であったが、「定期的な設定の見直し」を実施したことがないが 46.2%、「脆弱性（脅威、手口など）の最新情報取得」は 50.2%が実施したことがないという回答となり、半数程度の実施率であった。(本調査 問 13)

なお、構築年数による脆弱性対策の大きな変化はなかった。(問 7 と問 15)

これらから、実施も不実施も半数程度であり、仮説は必ずしも正しいとはいえない状況であることが伺われる。

(仮説 12) 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けるコストは変わらない

ウェブサイトの重要性・事業影響度の変化について尋ねたところ、「変わらない」という回答が 46.2%、「大幅に高まった」、「高まった」という回答の合計は 42.5%であり、「重要性が低下した」という回答は少なく、変わらないまたは重要性が高まったという回答が多い傾向にある。(本調査 問 6)

また、この 10 年程度のウェブサイトのセキュリティ対策コストの増減については、「変わらない」が 63.8%であり、この 10 年程度のウェブサイトの構築コストの増減についても「変わらない」が 58.8%、この 10 年程度のウェブサイトの運用コストの増減についても「変わらない」が 61.8%であった。(本調査 問 14、16、18)

これらから、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けるコストは変わらない結果であった。

(6)クラウド利用対策及び複数・複合的な対策

(仮説 13) 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

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るかについて尋ねた。全体としては、「明確になっている」が 49.7%と最も多いが、次いで「明確になっていない」が 36.9%との回答であり、委託先やサービス提供者との責任範囲は約 40%が明確になっていない状況であった。また、従業員数別でも同様の傾向であった。(本調査 問 4)

この結果から、仮説は必ずしも正しいとは言えないが、責任範囲が不明であり、自組織と委託先やサービス提供者のどちらで対応すべきか明確になっていない状況が伺える。

(仮説 14) 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

ウェブサイトの運用時に実施しているセキュリティ対策や脆弱性対策について尋ねたところ、問 15 で確認した 7 項目について、全項目で対策をしていない者は 24.9%、一つの対策を実施しているのは 4.3%、二つは 5.3%、三つは 7.0%、四つは 7.3%、五つは 6.6%、六つは 5.6%で、全項目を実施しているのは 38.9%であった。(問 15・複数対策)

この結果から、仮説は誤りであり、二つ以上の複数の対策が実施されていることが伺われる。

2.5.3. 企業規模による相違点について

従業員数 5 人以下の企業と 6～30 人の企業とでは、以下のような違いが見られる。

表 2.5.1　企業規模（従業員数）による相違点

項目	従業員数 5 人以下	従業員数 6～30 人
ウェブサイト構築・運用について（問 1、6）	・自社開発（オーサリング等利用）」が多い。 ・経営トップ自らが中心的役割を果たしている。	・外部委託による構築がより多い。 ・ウェブサイト担当者（責任者）を設けて経営者から指示。 ・ウェブサイトの重要性が高まっているがより高い。
ウェブサイトのセキュリティ対策（脆弱性対策）について（問 9、14、16、18、22）	・経営トップが判断。 ・セキュリティ対策、脆弱性対策に掛かるコストに変化がないがより多い。 ・脆弱性対策を判断する役割がきまっていないがより多い。 ・脆弱性の対処は、自社のウェブサイト管理者が多い。	・ウェブサイト担当者（責任者）が判断。 ・構築コスト・運用コストが増加した比率がより高い。 ・脆弱性の対処は、委託先やシステムベンダが多い。
セキュリティ対策の委託について（問 4）	・委託ルールが未整備（セキュリティ要件の指定の割合は低い）。	・委託ルールがしっかりしている（セキュリティ要件を指定している割合がより高い）。

2.5.4. 対策状況による相違点について

ウェブサイトの脆弱性対策を行っている企業等においては、対策を取っていない企業に比べ、組織的なセキュリティ管理が行われ、担当者や意思決定者が設定されている傾向が見られる。

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。

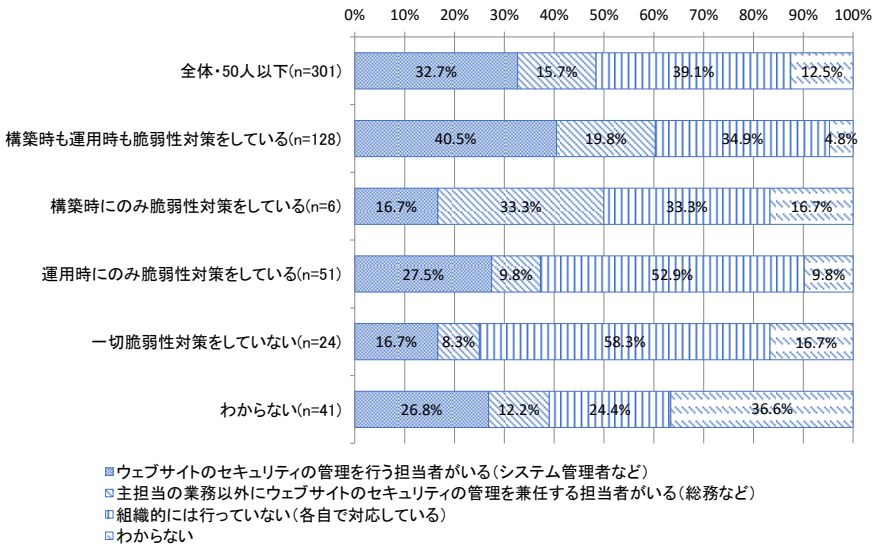

図 2.5.1 脆弱性対策状況 － 組織的セキュリティ管理の状況
（問 17、問 19 の集計結果と問 9）

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。

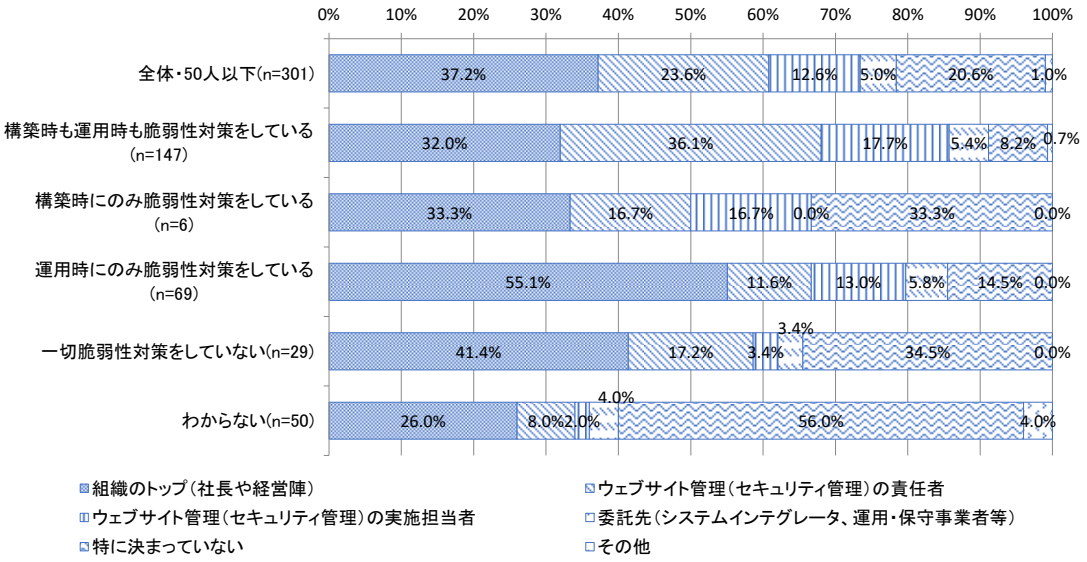

図 2.5.2 脆弱性対策状況 – セキュリティ対策の判断を行う人
（問 17、問 19 の集計結果と問 22）

2.5.5.2012 年度調査との経年変化について

2012 年度調査との経年変化は、2.4 節に記載したとおりであるが、これらの結果から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、及び IPA の施策課題について報告する。

(1)小規模ウェブサイト運営者の脆弱性対策等の変化

脆弱性対策が進んだ点及び変化が少なかった点について、脆弱性対策、組織体制の観点をまとめた内容を以下に示す。

表 2.5.2　脆弱性対策・組織体制の経年変化概要

	脆弱性対策	組織体制
進んだ点	・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）	・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いるが増加（問 9）
変化の少	・ウェブサイト運用時の脆弱性対策実	・ウェブサイトの運用・構築に関する組

なかった点	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）	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）

脆弱性対策が進んだ点は、ウェブサイトを開発・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）し、ウェブサイト構築時の脆弱性対策をしていないが減少した点（問 17）である。また、脆弱性対策や課題認識に変化の少なかった点は、ウェブサイトを運用する際の脆弱性対策の実施（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として、「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%、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%、「脆弱性やセキュリティに関する情報が多すぎて選別が難しい」は約 60%（問 26)。脆弱性対策・セキュリティ対策に関する IPA の各種資料の認知は約 60%から 80%が「聞いたことがない」という回答である（問 28)。
組織体制が進んだ点としては、「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」が減少し、「ウェブサイトのセキュリティ担当者がいる」が増加（ともに問 9）した点である。また、組織体制に変化が少なかった点は、ウェブサイトの運用・構築に関する組織トップ（社長や経営陣）の関与（問 5)、ウェブサイトの運用・構築を担当する方（ウェブサイト担当者）の選定理由(問 8)であったが、従業員 5 人以下の組織は「脆弱性対策を判断する役割が決まっていない」が増加（問 22）している。

(2)IPA の施策課題

IPA の施策課題として特に脆弱性対策の普及啓発とパートナーシップ制度の認知についてまとめた内容を以下に示す。

表 2.5.3　IPA の施策課題の概要

項目	内容
脆弱性対策の普及啓発	・ウェブサイトの脆弱性による被害や対策について「詳しく知っている」が減少、「知らなかった」が増加（問 11） ・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 70%が認知していない（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）
制度の認知	・「情報セキュリティ早期警戒パートナーシップ」の取組みを聞いたことがないが約 50%であり依然として高い（問 27）

脆弱性及び被害の理解促進については、ウェブサイトの脆弱性の理解として重要である被害や対策について詳しく知っているが減少し、知らなかったが増加（問 11）している。また、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に変化がない（問 28)。そのため、

ウェブサイトの脆弱性の理解や対策の重要性が普及啓発できていなく、脆弱性対策が進んでいない可能性がある。また、国内のウェブサイトへの脆弱性を悪用した攻撃等によって企業や組織が被害を受けていることを知った際に、それらの情報を参考にしたいが約 70%と高い状況（問 12）であるが、これらの情報を求めているウェブサイトの運営者に届いておらず、脆弱性の対策が進んでいない可能性がある。

制度運用については、「情報セキュリティ早期警戒パートナーシップ」の取組みを「聞いたことがある」は約 40%から 50%に増加したが、「聞いたことがない」は約 50%と高く（問 27)、脆弱性情報の届出を受け付け、コーディネーションを実施していることが認識されていない。

2.5.6.課題解決の検討

前述した課題を解決するために、小規模ウェブサイト運営者の意識、啓発、社会環境、制度運用等の各観点から検討した対策結果を以下に報告する。

(1)小規模ウェブサイト運営者の意識について

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として、「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運営者（重要な課題、課題のひとつのとの回答を合わせ）は約 70%、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」という回答は約 60%等と高い（問 26)。そのため、「企業ウェブサイトのための脆弱性対応ガイド」に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となる情報を集約し、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。

(2)啓発について

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）であるが、今回のアンケート調査結果で求められる情報を提供し、啓発を促進することが考えられる。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）ため、「企業ウェブサイトのための脆弱性対応ガイド」に具体的な被害情報を提供する必要がある。

(3)社会環境について

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」が増加している（問 3)。これらのことから、自組織のみで運用や対策を行うのではなく、外部サービスも利用することが多くなってきているため、「企業ウェブサイトのための脆弱性対応ガイド」に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がある。

(4)制度運用について

「情報セキュリティ早期警戒パートナーシップ」の取組みを「聞いたことがない」は 2012 年度

調査と今回調査で約 50%と高い（問 27）状態で変化がなく、脆弱性情報の届出を受け付け、コーディネーションしていることが広く認識されていない。パートナーシップの認知度を向上させ、望ましい脆弱性対処の方法についてウェブサイト運営者に認識させることで、パートナーシップでの対応がより早期に、より適切に実施できるようにすることが望ましい。

附録 1：アンケート調査項目

2020 年度 企業のウェブサイト運営に関する実態調査
アンケート調査票

予備調査 調査項目
■あなたの勤務先についてお伺いします。

予備調査 問 1
［全員に伺います］ あなたの勤務先の従業員数を教えてください。(1 つを選択)(役員、パート・アルバイト等を含めた人数でお答えください)

a. 1 ～ 5 人
b. 6 ～ 10 人
c. 11 ～ 15 人
d. 16 ～ 20 人
e. 21 ～ 25 人
f. 26 ～ 30 人
g. 31 ～ 50 人
h. 51 ～ 80 人
i. 81 人より多い

予備調査 問 2
あなたの勤務先の業種にあてはまるものを教えてください。(1 つを選択。複数ある場合は主な業種をお答えください)

a. 農林水産
b. 鉱業
c. 建設、土木、工事、プラント
d. 製造
e. 電気、ガス、熱供給、水道
f. 情報通信、IT 関連サービス
g. 新聞・出版・放送
h. 運輸、倉庫、郵便
i. 卸売
j. 小売
k. 金融、保険、投資、共済
l. 不動産
m. 研究開発・研究機関

n. 飲食店
o. 学校・教育
p. 保健・医療・福祉
q. 政府・地方公共団体・各種法人・団体等
r. その他のサービス

予備調査 問 3
あなたの勤務先の所在地にあてはまるものを教えてください。(1 つを選択)
a. 首都圏
b. 地方中枢都市（大阪圏、名古屋圏、及び札幌市、仙台市、広島市、福岡市、北九州市のいずれか）
c. 地方中枢都市以外の県庁所在地
d. 上記以外の人口 30 万人以上の都市
e. どれにもあてはまらない

■あなたの会社で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イト（ウェブサーバ、データベースサーバ等で構成されるものを想定）についてお伺いします。

予備調査 問 4
あなたが職務で関わっているウェブサイトの範囲についてあてはまるものを教えてください。(1 つを選択)
a. 自社のウェブサイトのみについて関わっている
b. 他社（顧客）のウェブサイトのみについて関わっている
c. 上の両方について関わっている
d. いずれにも関わっていない

予備調査 問 5
［自社のウェブサイトに関わっているとお答えの方（問 4 で a. あるいは c. を回答した方）にお尋ねします］ あなたが行っている自社のウェブサイトに関する業務について、あてはまるものをお答えください。(複数回答可)
a. 自社ウェブサイトの企画・発注（外注管理を含む）
b. 自社ウェブサイトの構築（外注を含まない）
c. 自社ウェブサイトの保守・運用・監視
d. 自社ウェブサイトを用いた広報・宣伝
e. 自社ウェブサイトを用いた販売

f. 自社ウェブサイトを用いた顧客サービス・サポート、顧客管理
g. 自社ウェブコンテンツの企画・制作
h. いずれにもあてはまらない

予備調査 問 6

［自社のウェブサイトに関わっているとお答えの方（問 4 で a. あるいは c. を回答した方）にお尋ねします］ あなたの会社ではどのような自社ウェブサイトを運営していますか。あてはまるものをお答えください。（複数回答可）

a. ウェブサイトのユーザの個人情報を扱っている（5000 件以上）
b. ウェブサイトのユーザの個人情報を扱っている（5000 件未満）
c. 企業案内
d. 製品・サービスの案内
e. 実店舗への誘導
f. 問い合わせ受付
g. インターネット通販、予約
h. コンテンツ販売・提供
i. 製品・サービスのキャンペーン（顧客との関係強化）
j. ポータル、メールマガジンの発行
k. ショッピング機能の提供
l. コミュニティ運営の代行（会員制 SNS、掲示板等）
m. アンケートの代行
n. その他（具体的に：　　）

予備調査 問 7

［他社（顧客）のウェブサイトに関わっているとお答えの方（問 4 で b. あるいは c. を回答した方）にお尋ねします］ あなたが行っている他社（顧客）のウェブサイトに関する業務について、あてはまるものをお答えください。（複数回答可）

a. 他社（顧客）のウェブサイトの構築
b. 他社（顧客）のウェブサイトの保守・運用・監視
c. 他社（顧客）のウェブコンテンツの企画・制作
d. いずれにもあてはまらない

予備調査 問 8

［他社（顧客）のウェブサイトに関わっているとお答えの方（問 4 で b. あるいは c. を回答した方）にお尋ねします］ あなたの会社ではどのような他社（顧客）のウェブサイトを扱っていますか。あてはまるものをお答えください。（複数回答可）

a. ウェブサイトのユーザの個人情報を扱っている（5000 件以上）

b. ウェブサイトのユーザの個人情報を扱っている（5000 件未満）
c. 企業案内
d. 製品・サービスの案内
e. 実店舗への誘導
f. 問い合わせ受付
g. インターネット通販、予約
h. コンテンツ販売・提供
i. 製品・サービスのキャンペーン（顧客との関係強化）
j. ポータル、メールマガジンの発行
k. ショッピング機能の提供
l. コミュニティ運営の代行（会員制 SNS、掲示板等）
m. アンケートの代行
n. その他（具体的に：　　）

予備調査 問 9

［全員に伺います］ もし、あなたの会社が関わっているウェブサイトにセキュリティに関するトラブルが生じたとき、あなたはどのように関与しますか。あてはまるものをお答えください。(1 つを選択)

a. 主にあなた自身がトラブルに対処する
b. 主に自社内の他の人が対処するが、あなたも関わる可能性がある
c. 自社内の他の人が対処し、あなたは関わらない
d. 委託先の事業者が対処し、あなたは報告を受ける
e. 委託先の事業者が対処し、あなたは関わらない
f. わからない

予備調査 問 10

あなたが関わるウェブサイトには以下のような機能・画面がありますか。あてはまるものすべてお答えください。(複数回答可)

a. ユーザ登録
b. 登録済みユーザのログイン
c. ユーザによるフォームへの入力（問合せ、掲示板等を含む）
d. 入力された情報の確認のための表示
e. ユーザへのメールの自動送信
f. サイト内の検索と結果表示
g. アクセスログやメール等の内容の画面表示
h. わからない

予備調査 問 11

あなたの会社での担当業務をお答えください。(1 つを選択)

a. 経営・経営企画
b. 総務・人事
c. 経理
d. 営業・販売
e. 広報・宣伝
f. 顧客サービス・サポート、顧客管理
g. 調査・マーケティング
h. 商品・サービス開発
i. 研究開発
j. 保守・運用・監視
k. 社内向けシステム・情報システム企画運用管理
l. ソリューション開発・設計
m. システム開発、システムエンジニア
n. ソフトウェア開発、プログラミング
o. システム企画・設計
p. システム運用管理・サーバー管理
q. データベース構築・運用
r. web サイト構築・管理
s. コンテンツ企画・制作
t. 生産・製造
u. 物流・輸送
v. 購買・調達
w. 教育・研修
x. その他（具体的に：　　）

本調査 調査項目

組織外とのやり取りに用いるウェブサイト

■貴社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イト（ウェブサーバ、データベースサーバ等で構成されるものを想定）についてお伺いします。

問1

[全員に伺います]

貴社で主要なウェブサイトを開発・構築した方法を教えてください。(1 つを選択)

a. 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）
b. 自社開発（自社で独自にウェブアプリケーションを開発し、構築）
c. 自社開発（既存のパッケージを利用・カスタマイズし、構築）
d. 外部事業者に構築を委託した
e. 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
f. 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
g. その他（具体的に：　　）
h. わからない

問2

貴社がウェブサイトを開発・構築する際、重視する点を教えてください。(複数選択可)

a. 費用
b. 納期（速さ）
c. 運用時の利便性・拡張性
d. セキュリティ
e. その他（具体的に：　　）
f. わからない

問3

貴社のウェブサイトの運用・管理の形態について教えてください。(1 つを選択)

a. 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全て運用・管理している
b. 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全て運用・管理している
c. 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。
d. 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
e. 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
f. 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
g. その他（具体的に：　　）

h. わからない

問4

[問 1 で e または f と回答した方、及び問 3 で c～f 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。(1 つを選択)

a. 明確になっている
b. 明確になっていない
c. その他 (具体的に :)
d. わからない

問5

ウェブサイトの運用・構築について、貴社のトップ(社長や経営陣)はどのように関与していますか。もっともあてはまるものをお答えください。(1 つを選択)

a. トップ自らがウェブサイトの運用・構築にあたっている
b. 積極的に担当者に指示を出し、ウェブサイトへの要望や意見も良く出している
c. ときどき担当者に指示を出し、報告も受けている
d. 担当者から報告を受けているが、基本的には担当者に任せている
e. その他 (具体的に :)
f. 特に関わっていない (担当者に一切を任せきりである)

問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は、どの様に変化しましたか。もっともあてはまるものをお答えください。(1 つを選択)

a. 大幅に高まった
b. 高まった
c. 変わらない
d. 低下した
e. 大幅に低下した
f. その他 (具体的に :)
g. わからない

問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。(1 つを選択)

a. 1 年未満
b. 1 年以上～5 年未満
c. 5 年以上～10 年未満

d. 10 年以上
e. わからない

問8

貴社のウェブサイトの運用・構築を担当する方（ウェブサイト担当者）は、どのような理由で選ばれていますか。あてはまるものを全てお答えください。（複数回答可）

a. パソコンに詳しい／パソコンに慣れているから
b. デザインができるから
c. プログラムができるから
d. 運営や管理ができるから
e. ウェブサイトのアクセス状況等の分析ができるから
f. ウェブサイトを使った販売等の担当だから
g. 広報の担当だから
h. その他（具体的に：　　）
i. 特にない

ウェブサイトのセキュリティ対策全般の状況

■貴社（会社、団体、機関等）におけるウェブサイトのセキュリティ対策全般の状況について伺います（ここで言うウェブサイトのセキュリティ対策には、ウイルス対策、個人情報漏洩への対策、ウェブサイトのトラフィックの監視、不正アクセスの検知、脆弱性対策などを含みます）。

問9

［全員に伺います］

貴社のウェブサイトのセキュリティ対策の管理は組織的に行っていますか。（複数回答可）

a. 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）
b. 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）
c. 組織的には行っていない（各自で対応している）
d. 一部を外部委託している
e. 大半を外部委託している
f. わからない

問10

［先の 問 9 で d または e と回答した方にお尋ねします］

外部委託の際にセキュリティ対策に関する要求事項（セキュリティ要件）をどの程度意識していますか。もっともあてはまるものをお答えください（1 つを選択）

a. セキュリティ要件については特に気にしていない

b. 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
c. セキュリティ要件は契約に含まれている
d. 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
e. その他（具体的に：　　）
f. わからない

貴社におけるウェブサイトの脆弱性に関する取組み

■貴社におけるウェブサイトの脆弱性に関する取組みについてお伺いします。

脆弱性（ぜいじゃくせい）とは

情報システムを狙う攻撃は情報システムに存在する情報セキュリティ上の「弱点」を突いて、情報システムに侵入したり、コンピュータウイルスを感染させることで行われます。このような情報システムの「弱点」は「脆弱性（ぜいじゃくせい)」と呼ばれています。新しい脆弱性は日々発見されており、これまで安全とされていた情報システムであっても安全であり続けるとは限りません。

以下の質問では、アプリケーション・ソフトウェアに関する脆弱性と、ミドルウェアや OS に関する脆弱性の両方についてお答えください。

問11

[全員に伺います]

ウェブサイトの脆弱性について、どの程度知っていましたか。あてはまるものをお答えください。(それぞれひとつを選択)

	詳しく知っている	聞いたことがある	知らなかった
(1) 「脆弱性」の種類とその内容	−	−	−
(a)SQL インジェクション	a.	b.	c.
(b)OS コマンド・インジェクション	a.	b.	c.
(c)パス名パラメータの未チェック／ディレクトリ・トラバーサル	a.	b.	c.
(d)セッション管理の不備	a.	b.	c.
(e)クロスサイト・スクリプティング	a.	b.	c.
(f)CSRF（クロスサイト・リクエスト・フォージェリ）	a.	b.	c.
(g)HTTP ヘッダ・インジェクション	a.	b.	c.
(h)アクセス制御や認可制御の欠落	a.	b.	c.
(2) ウェブサイトの脆弱性が原因で、重要な情報が盗まれたり、サービスを止められたりすることがある	a.	b.	c.
(3) ウェブサイトの脆弱性が原因で、ウェブサイトが迷惑メールや攻撃に悪用され、他の人に迷惑をかけることがある	a.	b.	c.
(4) ウェブサイトの脆弱性の根本的な対策は、プログラムの修正により脆弱性を無くすことである	a.	b.	c.

問12

国内のウェブサイトへの脆弱性を悪用した攻撃などによって企業や組織が被害を受けていることを知った時にどうしていますか。(1 つを選択)

a. 被害事例を参考に、自社のウェブサイトのセキュリティ対策を確認、見直し等をしている
b. 被害事例を参考に、対策をしたいが、十分に対応できていない
c. 被害事例は気になるが、何もしない
d. 被害事例は他人ごとなので、気にならない
e. その他（具体的に：　　）

問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。それぞれの項目であてはまるものを選択してください。(それぞれひとつを選択)

	実施している	実施したことはない
(1)　ソフトウェアの定期的な更新	a.	b.
(2)　セキュリティ製品利用	a.	b.
(3)　パスワードの管理・認証の強化	a.	b.
(4)　定期的な設定の見直し	a.	b.
(5)　脆弱性（脅威、手口など）の最新情報取得	a.	b.

問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。(1 つを選択)

a. 大幅に増加した
b. 増加した
c. 変わらない
d. 減少した
e. 大幅に減少した
f. その他（具体的に：　　）
g. わからない

問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。(それぞれひとつを選択)

	頻繁に実施する	たまに実施する	実施したことはない
(1) ウェブサーバ上で動作するアプリケーションの脆弱性対策（パッチ適用やバージョンアップ）	a.	b.	c.
(2) サーバソフトウェア・ミドルウェアの脆弱性対策（パッチ適用やバージョンアップ）	a.	b.	c.
(3) ウェブサーバの OS の脆弱性対策（パッチ適用やバージョンアップ）	a.	b.	c.
(4) 利用しているネットワーク機器の脆弱性対策（パッチ適用やバージョンアップ）	a.	b.	c.
(5) セキュリティ製品の導入や更改	a.	b.	c.
(6) セキュリティ診断	a.	b.	c.
(7) 不正な通信の遮断、通信のフィルタリング	a.	b.	c.

問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。(1 つを選択)

a. 大幅に増加した
b. 増加した
c. 変わらない
d. 減少した
e. 大幅に減少した
f. その他（具体的に：　　）
g. わからない

問17

貴社ではウェブサイトを構築する際に、どのような脆弱性対策を実施していますか。あてはまるものを全てお答えください。(複数回答可)

a. 仕様に脆弱性対策に関する項目を含めている
b. 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
c. 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
d. 構築が完成に近づいたら脆弱性検査や診断を行っている
e. 納品時に脆弱性対策に関する仕様項目について検査をしている
f. 構築の時点では脆弱性対策はしていない
g. その他（具体的に：　　）
h. わからない

問18

この 10 年くらいで、貴社のウェブサイト運用(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。(1 つを選択)

a. 大幅に増加した
b. 増加した
c. 変わらない
d. 減少した
e. 大幅に減少した
f. その他（具体的に：　　）
g. わからない

問19

貴社ではウェブサイトを運用するにあたり、どのような脆弱性対策を実施していますか。あてはまるものを全てお答えください。（複数回答可）

a. 脆弱性が発見されたら、可能な限り速やかに修正を行っている
b. 脆弱性が発見されたら、問題が生じない限りは運用を続け、修正する機会があれば直す
c. 脆弱性が発見されたら、その深刻さについて調べ、対処方法を検討する
d. 脆弱性が発見されたら、修正はしないが問題となる機能・画面を使わせないようにする
e. 脆弱性が発見されたら、修正はしないがセキュリティ製品（WAF など）で防御する
f. 定期的に脆弱性検査や診断を行っている
g. ウェブサイトを構成するソフトウェア等の脆弱性について情報収集を行っている
h. 運用における脆弱性対策はしていない
i. その他（具体的に：　　）
j. わからない

問20

［先の 問 17 で f と回答した方 または 問 19 で h と回答した方にお尋ねします］
脆弱性対策を行わない理由を教えてください。あてはまるものを全てお答えください。（複数回答可）

a. 個人情報を扱っていないから
b. クレジットカード等の決済を行なっていないから
c. サイトが著名でないので、被害に遭うとは考えにくいから
d. 深刻な問題ではないから
e. 難しくてよくわからないから
f. あまり気にしていないから
g. 脆弱性について知らなかったから
h. その他（具体的に：　　）
i. わからない

問21

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気付いた、きっかけは何ですか。あてはまるものを全てお答えください。（複数回答可）

a. ウェブサイトの利用者から連絡を受けた
b. 社外の関係者や取引先等から連絡を受けた
c. システムインテグレータやシステム販社、運用・保守事業者から連絡を受けた
d. セキュリティ関連組織等から連絡を受けた
e. 脆弱性検査や脆弱性診断サービスを通じて発見した
f. 脆弱性による情報を入手して、自社で確認し発見した
g. ウイルス・ワームや不正アクセスの被害が発覚し、その原因分析時に発見した
h. 動作にトラブル等があり確認したところ不具合とともに脆弱性に発見した
i. その他（具体的に：　　）
j. 脆弱性が見つかったことはない
k. わからない

問22

ウェブサイトの脆弱性対策などのセキュリティ対策について、対策を適用すべきか否か等を判断する人は誰ですか。（判断とは、承認行為ではなく、諸事情を考慮して対処の内容を決める行為とします）（1 つを選択）

a. 組織のトップ（社長や経営陣）
b. ウェブサイト管理（セキュリティ管理）の責任者
c. ウェブサイト管理（セキュリティ管理）の実施担当者
d. 委託先（システムインテグレータ、運用・保守事業者等）
e. その他（具体的に：　　）
f. 特に決まっていない

問23

貴社では、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、改ざん、不正アクセス、サーバのダウン等の被害に遭った経験はありますか。（1 つを選択）

a. 業務に影響が生じる被害が発生したことがある
b. 被害に遭ったことはあるが実害が発生したことはない
c. 被害に遭った経験はない
d. わからない

問24

もし運用中のウェブサイトについて脆弱性が発見された場合には、ウェブサイトの一時停止、該当箇所の修正、回避策の適用等（含テスト）の作業は誰が担当しますか。（1 つを選択）

a. ウェブサイト管理（セキュリティ管理）の実施担当者
b. 委託先のシステムインテグレータや運用・保守事業者
c. 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
d. 特に脆弱性対策は取らない
e. その他（具体的に：　　）
f. わからない

問25

ウェブサイトの脆弱性対策・セキュリティ対策に必要な費用や人員はどの程度確保されていますか。（1 つを選択）

a. 十分に確保できている
b. おおむね確保できている
c. やや不足している
d. 全く足りていない
e. わからない

貴社におけるウェブサイトの脆弱性対策（セキュリティ対策）に関する課題

■貴社におけるウェブサイトの脆弱性対策（セキュリティ対策）に関する課題についてお伺いします。

問26

[全員に伺います]

貴社の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について、それぞれの項目であてはまるものを選択してください。（それぞれ 1 つを選択）

	重要な課題である	課題のひとつである	特に課題ではない
(1) 対策を行うための予算が確保できない	a.	b.	c.
(2) 脆弱性やセキュリティに関する技術の習得が難しい	a.	b.	c.
(3) 対策を行うための人員が足りない	a.	b.	c.
(4) 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	a.	b.	c.
(5) 脆弱性やセキュリティに関する情報が多すぎて選別が難しい	a.	b.	c.
(6) 脆弱性を修正すると、ウェブ上のアプリケーションが動かなくなる可能性がある	a.	b.	c.
(7) 脆弱性対策の実施について判断できる人がいない	a.	b.	c.
(8) 脆弱性の問題でサービスを止めると、顧客を失ってしまう	a.	b.	c.
(9) 脆弱性対策やセキュリティ対策について組織トップの理解を得ることが難しい	a.	b.	c.
(10) 脆弱性対策やセキュリティ対策について社内ユーザーの理解を得ることが難しい	a.	b.	c.
(11) その他（具体的に：　　）	a.	b.	c.

脆弱性対策に関する公的な取組みの認知状況

■脆弱性対策に関する公的な取組みの認知状況についてお伺いします

独立行政法人情報処理推進機構（IPA）では、「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）の告示を踏まえ、ソフトウエア製品及びウェブアプリケーションの脆弱性に関する届出を受け付けています。IPA は調整機関である JPCERT/CC と連携し、日本国内における脆弱性情報の適切な流通に取組んでいます。この基準をふまえ、IPA、JPCERT/CC、一般社団法人 電子情報技術産業協会（JEITA）、一般社団法人 情報サービス産業協会（JISA）、一般社団法人コンピュータソフトウェア協会（CSAJ）、特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）は共同で、脆弱性関連情報の流通に関わる関係者、関係業界としての指針「情報セキュリティ早期警戒パートナーシップガイドライン」を作成しています。

問27

[全員に伺います]

これまでに上記の「情報セキュリティ早期警戒パートナーシップ」の取組みについてご存知でしたか。（1 つを選択）

a. 実際に脆弱性について通知を受けたことがある
b. 聞いたことがあり、内容も良く知っている
c. 聞いたことがあるが、内容は良く知らない
d. 聞いたことはない

脆弱性対策および情報セキュリティ対策に関するコンテンツ等の普及状況

■脆弱性対策および情報セキュリティ対策に関するコンテンツ等の普及状況についてお伺いします

問28

[全員に伺います]

脆弱性対策・セキュリティ対策に関する次の情報について知っていますか。(それぞれ 1 つを選択)

		参考にしている	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
(1)	「安全なウェブサイトの作り方」 https://www.ipa.go.jp/security/vuln/websecurity.html	a.	b.	c.	d.
(2)	「安全な SQL の呼び出し方」 https://www.ipa.go.jp/security/vuln/websecurity.html#sql	a.	b.	c.	d.
(3)	「Web Application Firewall 読本」 https://www.ipa.go.jp/security/vuln/waf.html	a.	b.	c.	d.
(4)	安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～ https://www.ipa.go.jp/security/vuln/websitecheck.html	a.	b.	c.	d.
(5)	ウェブサイト運営者のための脆弱性対応ガイド https://www.ipa.go.jp/files/000058492.pdf	a.	b.	c.	d.
(6)	知っていますか？ 脆弱性（ぜいじゃくせい） ―アニメで見るウェブサイトの脅威と仕組み― https://www.ipa.go.jp/security/vuln/vuln_contents/index.html	a.	b.	c.	d.
(7)	脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes） https://jvn.jp/	a.	b.	c.	d.
(8)	脆弱性対策情報データベース JVN iPedia https://jvndb.jvn.jp/	a.	b.	c.	d.
(9)	脆弱性対策情報共有フレームワーク MyJVN （MyJVN バージョンチェッカ） https://jvndb.jvn.jp/apis/myjvn/	a.	b.	c.	d.
(10)	中小企業向け情報セキュリティ対策ツール （5 分でできる！自社診断シート、中小企業の情報セキュリティガイドライン） https://www.ipa.go.jp/security/manager/know/sme-guide/index.html	a.	b.	c.	d.
(11)	安全なウェブサイト運営にむけて ～ 企業ウェブサイトのための脆弱性対応ガイド ～ https://www.ipa.go.jp/security/ciadr/safewebmanage.pdf	a.	b.	c.	d.
(12)	ウェブサイト構築事業者のための脆弱性対応ガイド ～ウェブサイト構築にかかわるすべての人に～ https://www.ipa.go.jp/files/000058491.pdf	a.	b.	c.	d.
(13)	IPA テクニカルウォッチ 「ウェブサイト開設等における運営形態の選定方法に関する手引き」 https://www.ipa.go.jp/security/technicalwatch/20180530.html	a.	b.	c.	d.
(14)	ウェブサイト運営のファーストステップ ～ウェブサイト運営者がまず知っておくべき脅威と責任～ https://www.ipa.go.jp/files/000071949.pdf	a.	b.	c.	d.
(15)	中小企業の情報セキュリティ対策ガイドライン 付録 6： クラウドサービス安全利用の手引き https://www.ipa.go.jp/files/000072150.pdf	a.	b.	c.	d.
(16)	その他（具体的に：　　）	a.	b.	c.	d.

問29

情報セキュリティに関してどのような普及・啓発コンテンツを利用してみたいですか（複数選択可）

a. ウェブサイトのセキュリティ対策の運用・管理に関するコンテンツ
b. セキュアなウェブサイトの構築に関するコンテンツ
c. セキュアなウェブサイトを発注するための要件が分かるコンテンツ
d. 最近のウェブサイトに関するセキュリティ脅威の動向が分かるコンテンツ
e. その他（具体的に：　　）
f. とくにない

附録 2：2012 年度アンケート調査項目との対比表

2020 年度調査		2012 度年調査	備考
予備調査 問 1	⇔	予備調査 問 1	
予備調査 問 2	⇔	予備調査 問 2	
予備調査 問 3	⇔	予備調査 問 3	
予備調査 問 4	⇔	予備調査 問 4	
予備調査 問 5	⇔	予備調査 問 5	
予備調査 問 6	⇔	予備調査 問 6	
予備調査 問 7	⇔	予備調査 問 7	
予備調査 問 8	⇔	予備調査 問 8	
予備調査 問 9	⇔	予備調査 問 9	
予備調査 問 10	⇔	予備調査 問 10	
予備調査 問 11	⇔	予備調査 問 11	
本調査 問 1	⇔	本調査 問 1	
本調査 問 2	⇔	本調査 問 2	
本調査 問 3	⇔	本調査 問 3	
本調査 問 4（新設）	⇔	本調査 問 4（削除）	※別設問
本調査 問 5	⇔	本調査 問 5	
本調査 問 6（新設）	⇔	—	
本調査 問 7（新設）	⇔	—	
本調査 問 8	⇔	本調査 問 6	
本調査 問 9	⇔	本調査 問 7/8	※項目の一部同一
本調査 問 10	⇔	本調査 問 9	
—	⇔	本調査 問 10（削除）	
本調査 問 11	⇔	本調査 問 11	※項目の一部同一
本調査 問 12（新設）	⇔	—	
本調査 問 13（新設）	⇔	—	
本調査 問 14（新設）	⇔	—	
本調査 問 15（新設）	⇔	—	
本調査 問 16（新設）	⇔	—	
本調査 問 17	⇔	本調査 問 12	
本調査 問 18（新設）	⇔	—	
本調査 問 19	⇔	本調査 問 13	
本調査 問 20	⇔	本調査 問 14	
本調査 問 21	⇔	本調査 問 15	

本調査 問 22	⇔	本調査 問 16	
本調査 問 23	⇔	本調査 問 17	
本調査 問 24	⇔	本調査 問 18	
本調査 問 25	⇔	本調査 問 19	
本調査 問 26	⇔	本調査 問 20	
本調査 問 27	⇔	本調査 問 21	
本調査 問 28	⇔	本調査 問 22	
―	⇔	本調査 問 23（削除）	
本調査 問 29	⇔	本調査 問 24	