小企業における脆弱性対応の実態に関する調査報告書

2013 年 3 月

IPA 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

一般に、小企業においては、予算や人手が十分でなく、適切な脆弱性対策の実施は容易でないと考えられる。そのため、現在、IPA において受け付けているウェブサイトの脆弱性届出では、小企業のウェブサイトが大きな割合を占めている。

小企業においても B2C ビジネスにウェブサイトを活用することは一般的であり、脆弱性を放置すると、不特定多数の一般ユーザを危険な状態に陥れることになる。また、小企業であっても、発注元のウェブサイト（例：アンケート、キャンペーン等の一時的なサイト）の構築・運用を請け負うケースがあり、小企業の無理解が発注元のリスクに直結する可能性もある。さらに、ウェブサイトにマルウェアを仕込まれて、サイトの訪問者に感染させてしまう事態も考えられる。したがって、小企業のウェブサイトの脆弱性対策は喫緊の課題であり、効果的な促進策を適用することが求められる。

このような背景のもと、小企業に向けウェブサイト脆弱性対策に関する効果的な啓発を行うことを目指し、ウェブサイト運営およびセキュリティ対策の状況について実態を把握するための以下の調査を実施した。

(1) 小企業のウェブサイト運営に関するアンケート調査

(2) 小企業ウェブサイトの運営者及び関係者に対するヒアリング調査

これらの実態調査の結果は、小企業の経営者やウェブサイト担当者が脆弱性対策について正しく理解するための啓発資料作成に資するものとする。

1.2. 調査手法

(1) アンケート調査

小企業における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) ヒアリング調査

(1)の結果を踏まえ、脆弱性対策を促すための方策やその普及方策について、小企業のウェブサイト運営者や関係者にヒアリング調査を行った。

調査対象となる小企業のウェブサイト運営者は、(1)のアンケート回答者から抽出した。

また、(1)の結果の解釈や普及啓発の方策について意見を得るため、小企業のウェブサイト構築・運用を支援する事業者等の業界団体の関係者にも調査対象とした。

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。

[調査方法]　ウェブ・アンケート調査（企業モニター）

[調査対象]

・国内の小企業のウェブサイト担当者や情報システム担当者（本調査は 310 件が対象）。

・対象者は、小企業（従業員数 30 人未満、卸売業・小売業（飲食店を 含む）・サービス業で従業員 10 人未満の企業）に所属し、「自組織のシステムの企画・構築・運用・保守」および「情報セキュリティに関わる業務」に関与している者とする。

[有効回収数]　243 件（本調査）

[調査実施期間] 2012 年 12 月～2013 年 1 月

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・運用の実態

（２）ウェブサイトの脆弱性対策に関する理解

（３）ウェブサイトのセキュリティ対策／脆弱性対策の現状

（４）脆弱性対策に関する課題

（５）脆弱性およびセキュリティ対策関連事業等に関する認知度

2.3.調査分析の方針

アンケート調査に関しては、10 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 7 「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 19 「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 16 「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構築段階の対策が全てでその後は検討や改善は殆ど行っていない

→ 本調査 問 12 「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 13 「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 14 「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 14 「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 20(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 20(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 20(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 19「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 20(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 20(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 6「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 20(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 13「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 17「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 18「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 21「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 22「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」

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」(50.9%) が最も多く、「6～10 人」(22.3%)、「16～20 人」(8.8%) が続く。

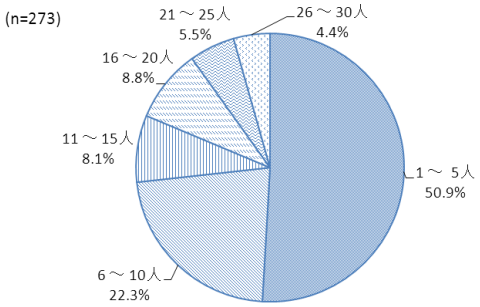

図 2.4.1 回答者の所属する企業等の従業員数（予備調査 問 1）

(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」(34.5%) が最も多く、「情報通信、IT 関連サービス」(27.5%)、「小売」(8.1%)、「製造」(5.5%) が続く。

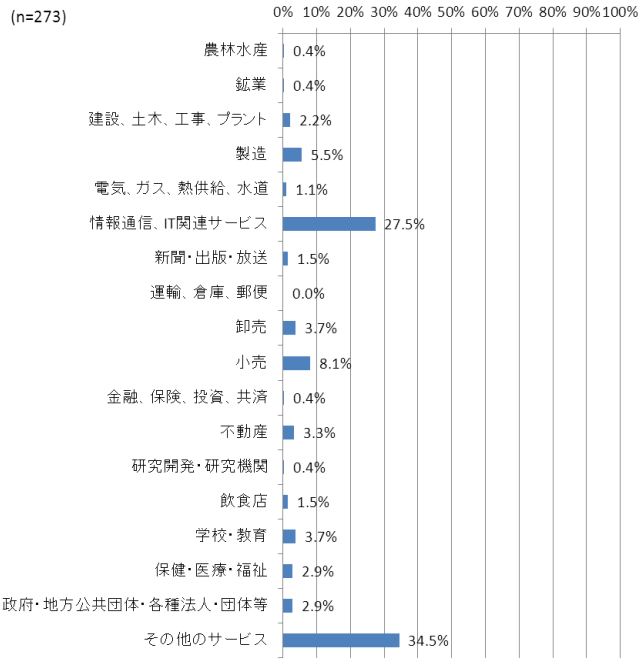

図 2.4.2 回答者の所属する企業等の業種（予備調査 問 2）

(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 42.1%、「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。

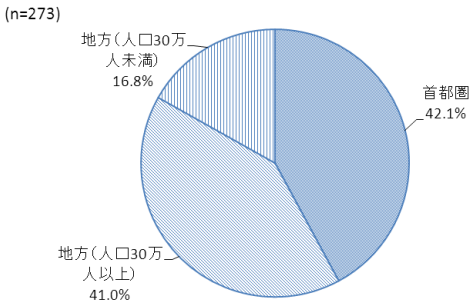

図 2.4.3 回答者の所属する企業等の所在地（予備調査 問 3）

(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」(40.9%)、「顧客サービス・サポート、顧客管理」(22.0%)、「広報・宣伝」(17.6%)、「コンテンツ企画、制作」(13.6%)、「社内向けシステム・情報システム企画運用管理」(5.9%) であった。

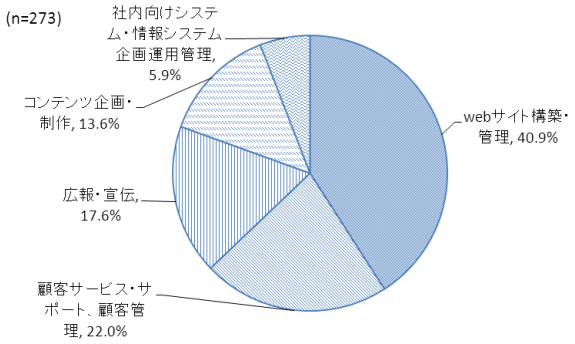

図 2.4.4 回答者が担当する業務（予備調査 問 11）

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。他社（顧客）のウェブサイトに関わっている回答者は全体の 42.9%であった。

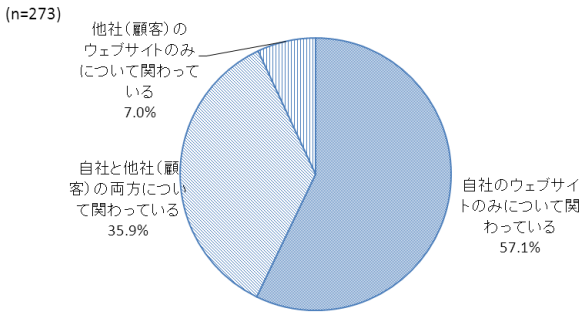

図 2.4.5 職務で関わっているウェブサイトの範囲（予備調査 問 4）

(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」(59.1%)、「自社ウェブコンテンツの企画・制作」(55.1%)、「自社ウェブサイトの構築（外注を含まない）」(52.0%)、「自社ウェブサイトを用いた広報・宣伝」(47.2%) が上位を占めた。

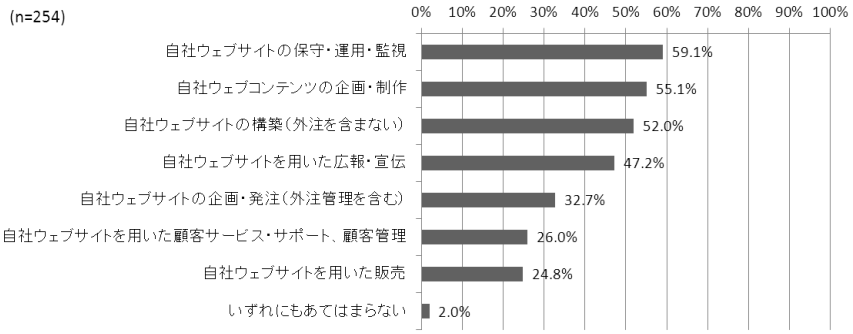

図 2.4.6 自社ウェブサイトに関する回答者の業務（予備調査 問 5）

(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（73.5%）、「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 6 割を超えた。

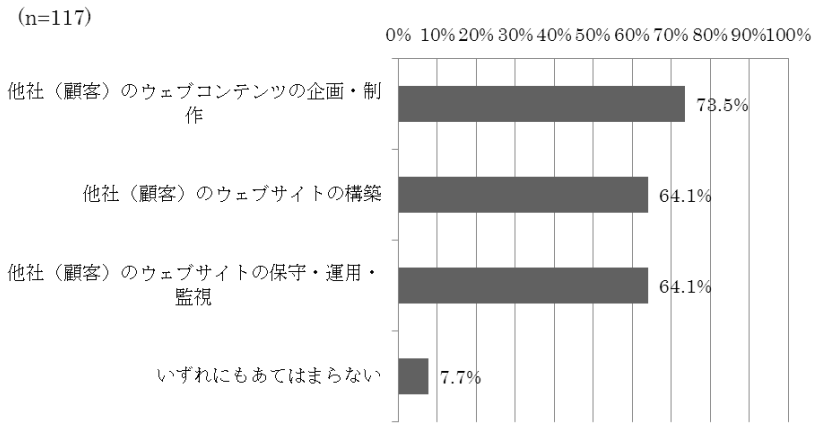

図 2.4.7 顧客ウェブサイトに関する回答者の業務（予備調査 問 7）

(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 49.5%と約半数を占めた。

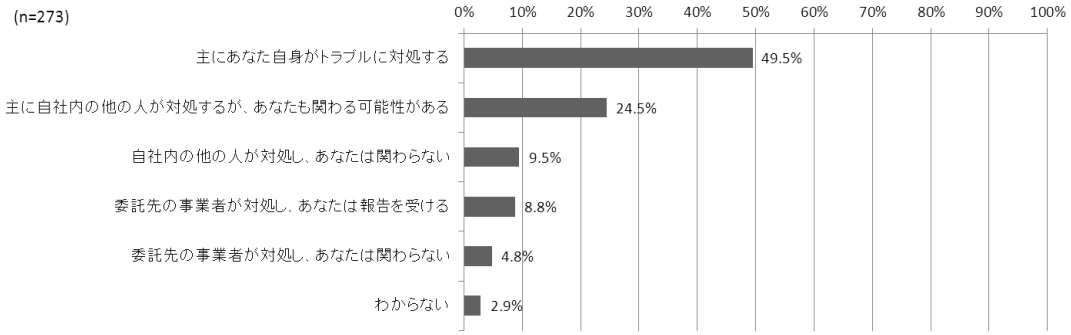

図 2.4.8 ウェブサイトでトラブルが発生した際の回答者の関与（予備調査 問 9）

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）。「企業案内」（64.6%）、「製品・サービスの案内」（63.8%）、「問い合わせ受付」（55.9%）が上位を占めた。

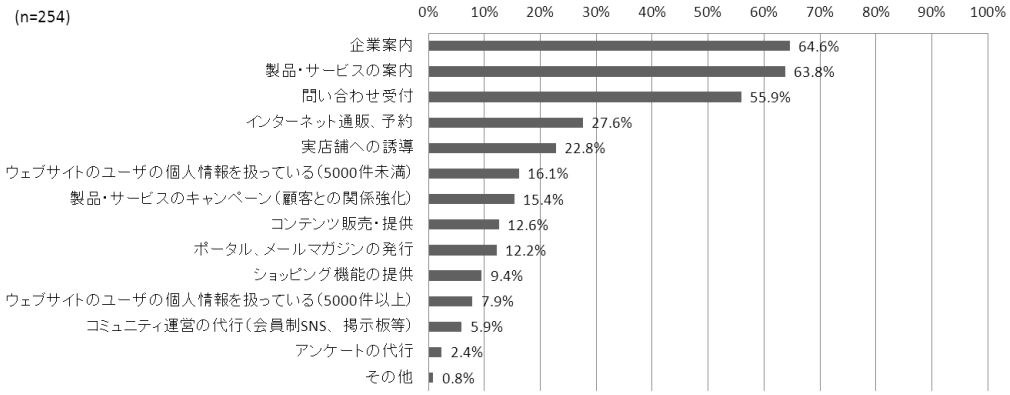

図 2.4.9 自社ウェブサイトの特徴（予備調査 問 6）

(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）。「企業案内」（71.8%）、「製品・サービスの案内」（65.8%）、「問い合わせ受付」（49.6%）が上位を占めた。

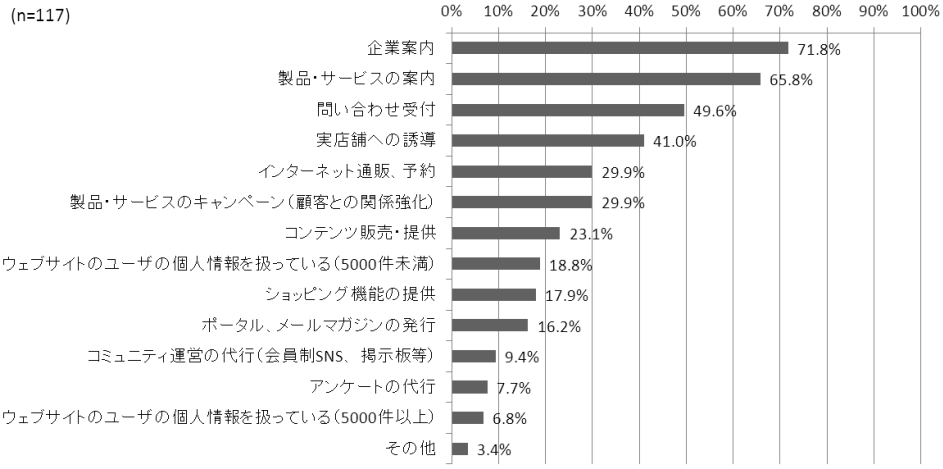

図 2.4.10 顧客ウェブサイトの特徴（予備調査 問 8）

(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）」（55.7%）、「入力された情報の確認のための表示」（40.7%）、「ユーザへのメールの自動送信」（40.7%）が上位を占めた。

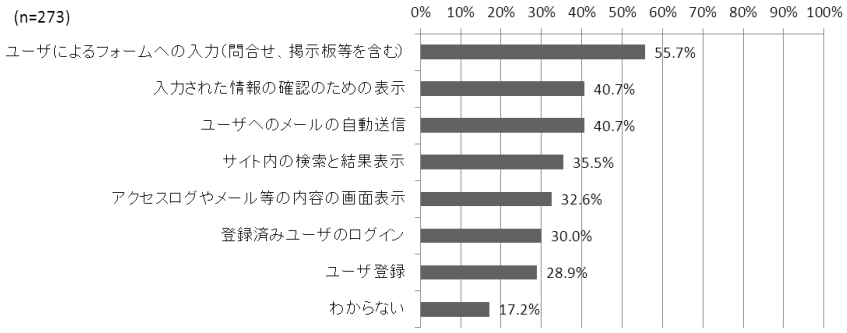

図 2.4.11 ウェブサイトが備える機能・画面（予備調査 問 10）

(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。自社での開発・構築がおよそ過半数を占めた。

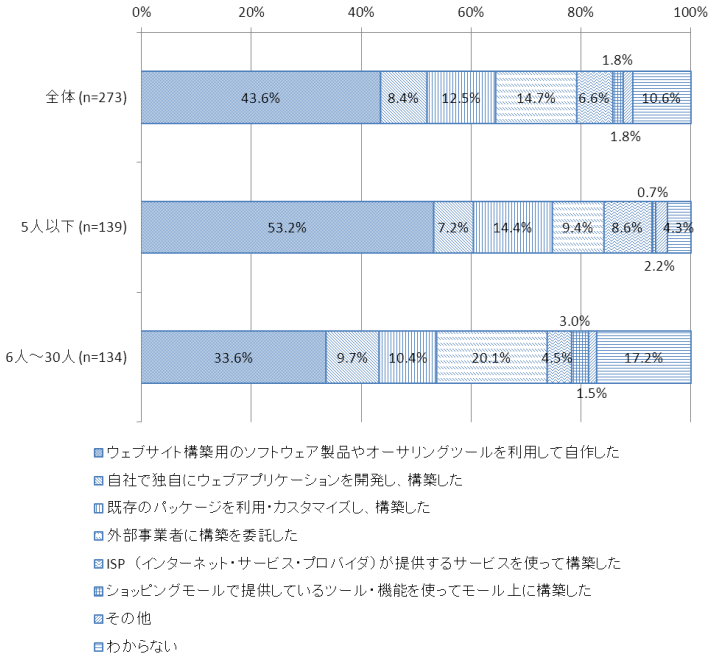

図 2.4.12 開発・構築の方法（本調査 問 1）

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

(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」（73.3%）、「運用時の利便性・拡張性」（63.4%）が上位を占めた。

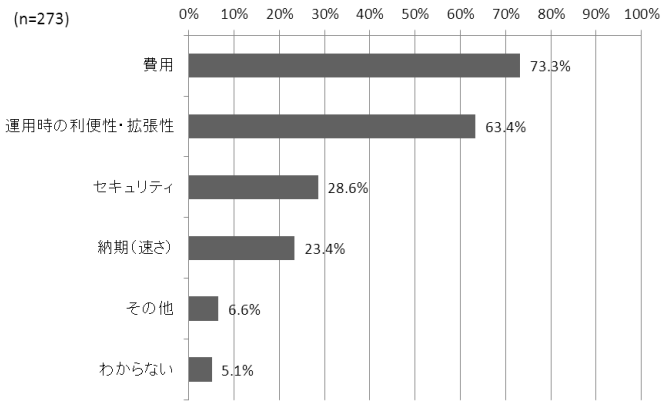

図 2.4.13 開発・構築の際に重視する点（本調査 問 2）

(5) 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 42.8%であった。外部のサービス（ホスティング、クラウド、ASP サービス、ショッピングモール）を利用しているという回答は合わせて全体の 47.3%であった。

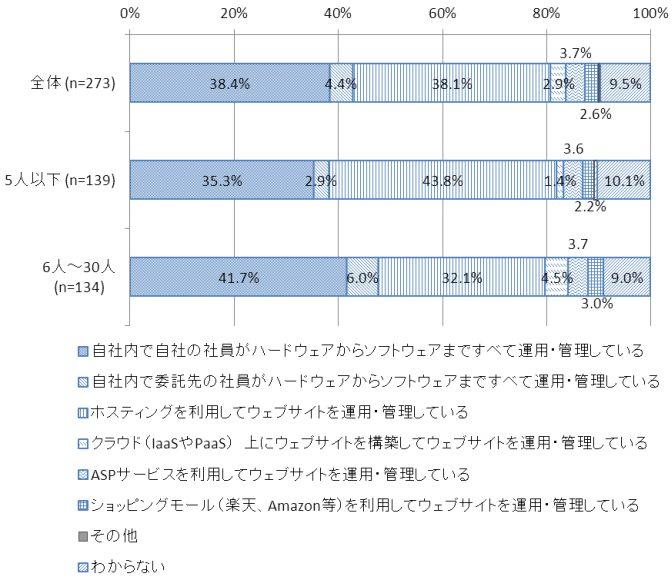

図 2.4.14 運用・管理の形態（本調査 問 3）

(b) 保守・運用の委託

ウェブサイトの保守・運用を委託していると回答した者に、その内容についてあてはまるものを質問した（複数回答可）。システム保守を委託しているという回答が 64.8%と過半数であった。

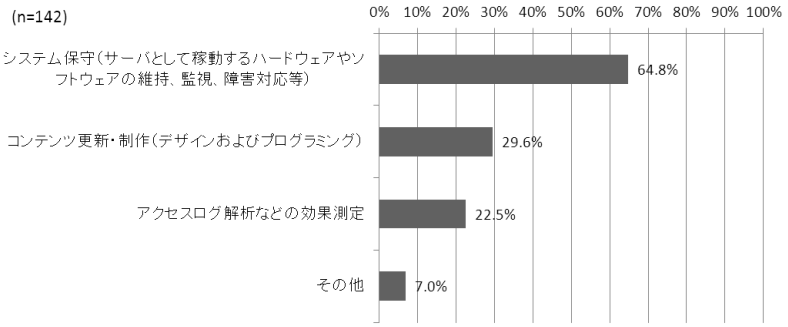

図 2.4.15 保守・運用の委託（本調査 問 4）

(6) 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。「トップ自らがウェブサイトの運用・構築にあたっている」との回答は全体の 35.4%であった。

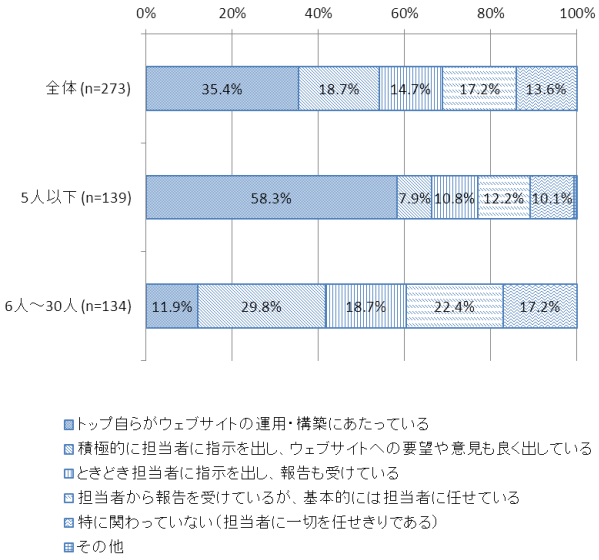

図 2.4.16 経営層の関与（本調査 問 5）

(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」（60.8%）、「デザインができるから」（46.5%）、「運営や管理ができるから」（44.7%）が上位を占めた。

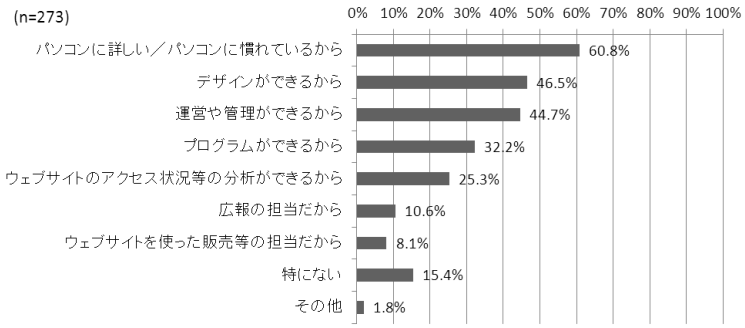

図 2.4.17 ウェブサイト担当者を選ぶ観点（本調査 問 6）

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 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%であった。

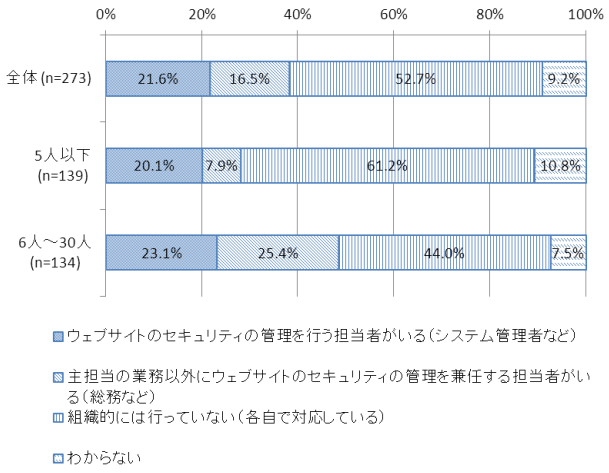

図 2.4.18 組織的なセキュリティ管理（本調査 問 7）

(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尋ねた。「大半を組織内で実施している」との回答は全体の 53.1%、一部あるいは大半を委託しているとの回答は合わせて全体の 31.5%であった。

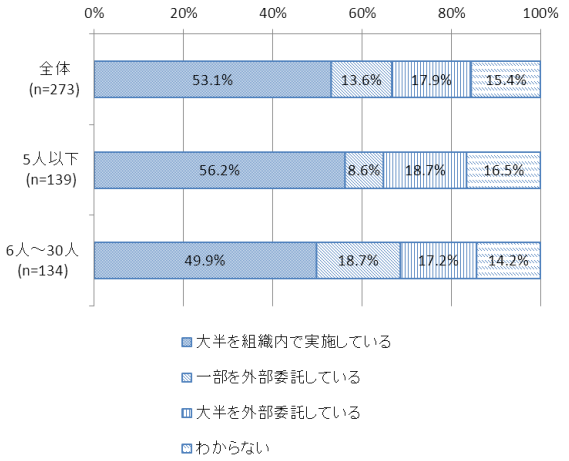

図 2.4.19 外部委託の実施（本調査 問 8）

(b)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。

「特に気にしていない」とする回答は全体の 14.0%であった。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全体の 42.9%であった。

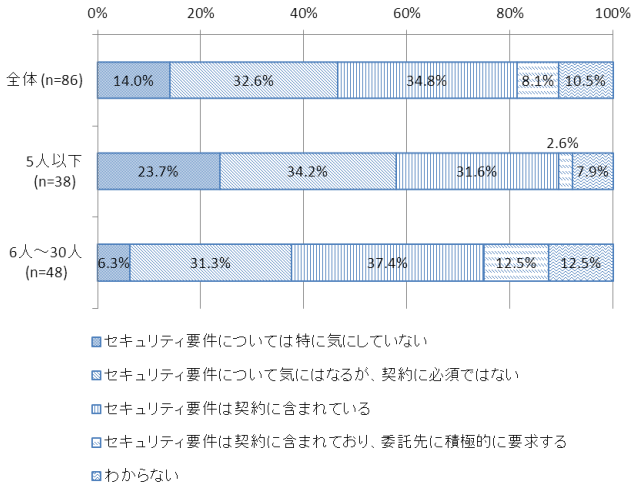

図 2.4.20 セキュリティ要件（本調査 問 9）

(c)報告文書の取得

外部委託を行っていると回答した者に、委託先から具体的なセキュリティ対策についての報告文書を取得しているかをを質問した。

セキュリティ対策について何らかの文書を委託先から取得しているとする回答は合わせて全体の 34.9%であった。報告文書を取得していないとする回答は全体の 53.5%であった。

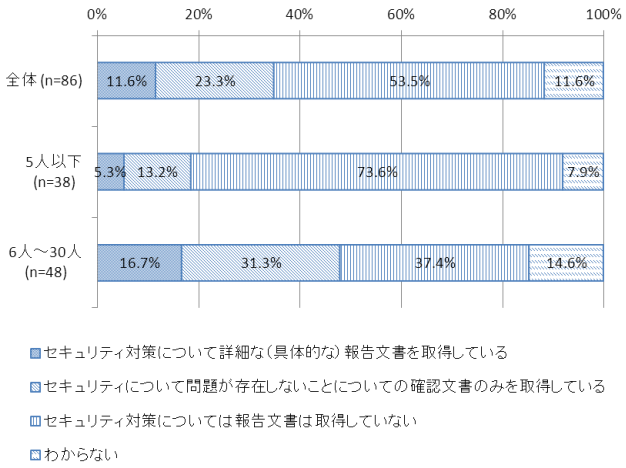

図 2.4.21 報告文書の取得（本調査 問 10）

2.4.5. ウェブサイトの脆弱性対策の状況について

(1) ウェブサイト脆弱性の認知度

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。全体の 5 割から 6 割が詳しく知っているとの回答が得られた。

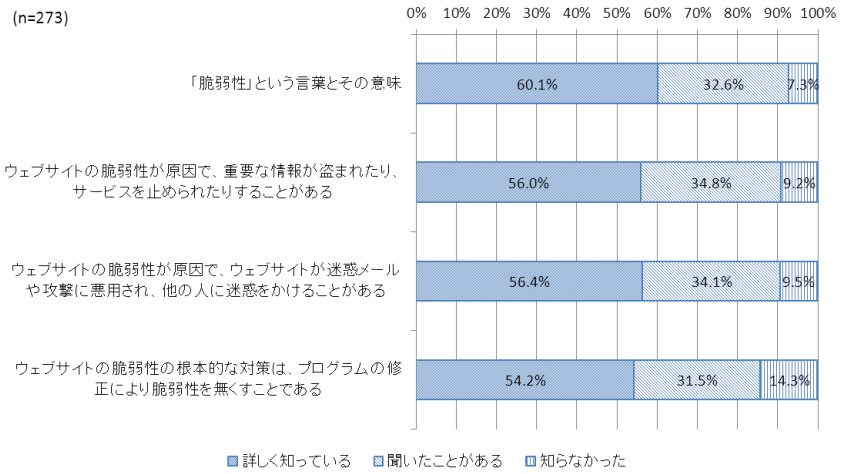

図 2.4.22 ウェブサイト脆弱性の認知度（本調査 問 11）

(2) 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）。構築に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 37.0%であった。

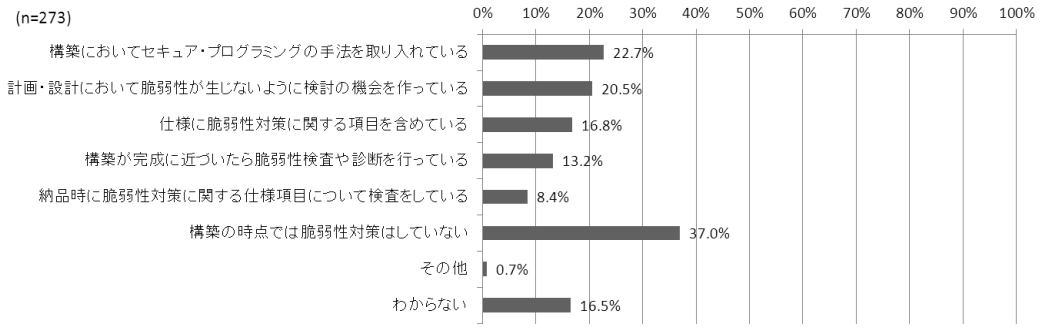

図 2.4.23 構築時の脆弱性対策の内容（本調査 問 12）

(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）。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 17.2%であった。

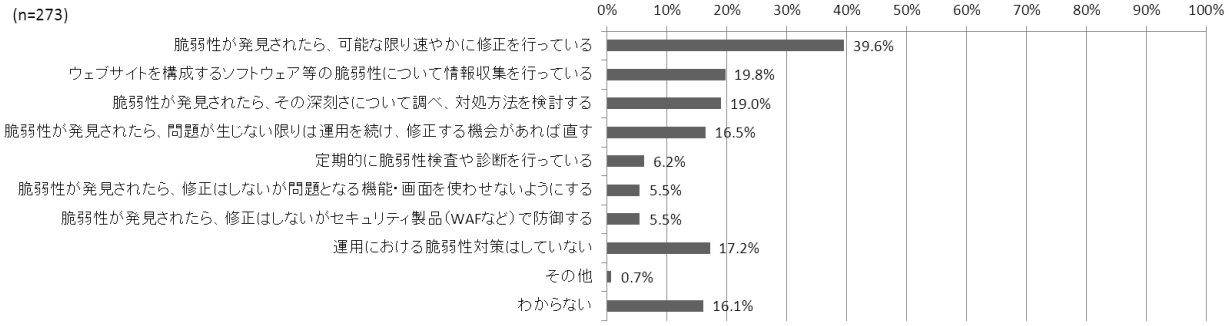

図 2.4.24 運用時の脆弱性対策の内容（本調査 問 13）

(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（いずれかの設問でわからないとした回答は全て「わからない」に集約している）。

構築時と運用時のいずれでも脆弱性対策をしているとした回答者は全体の 45.4%であった。いずれについても脆弱性対策はしていないとした回答者は全体の 16.8%であった。

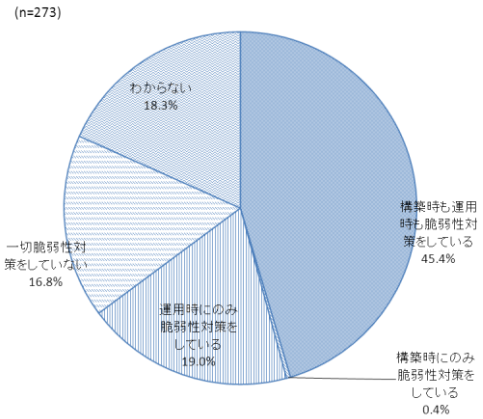

図 2.4.25 脆弱性対策の実施状況（本調査 問 12 および問 13）

(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）。

「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た。

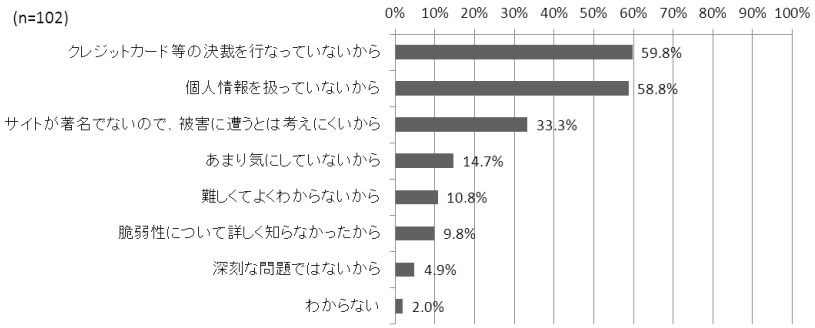

図 2.4.26 脆弱性対策を行わない理由（本調査 問 14）

(3) 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）。「脆弱性がみつかったことはない」とする回答は全体の 54.2%であった。特に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全体の 20.1%であった。

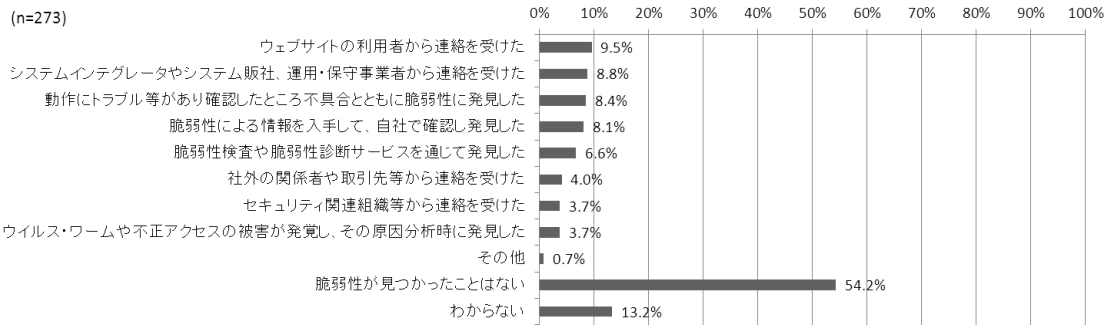

図 2.4.27 脆弱性に気付いたきっかけ（本調査 問 15）

(4) 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。被害の経験があると答えた回答は全体の 15.1%であった。

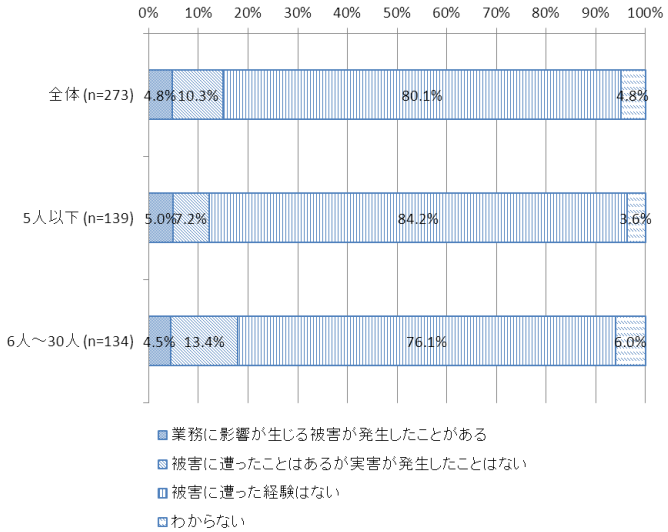

図 2.4.28 脆弱性に起因する被害の経験（本調査 問 17）

(5) 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。確保できているという回答は全体の 44.0%、不足しているという回答は全体の 36.6%であった。

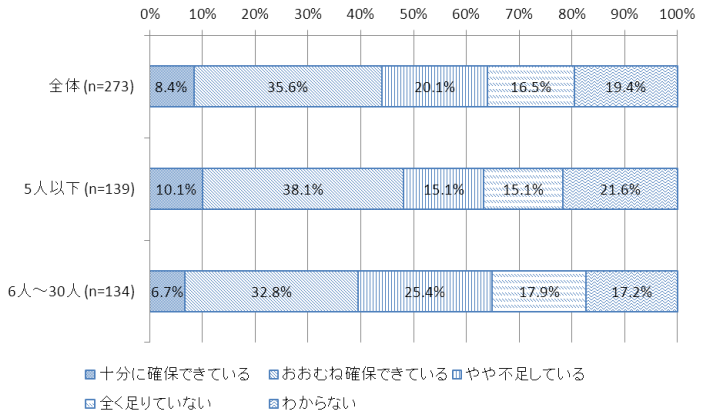

図 2.4.29 セキュリティ対策（脆弱性対策）の費用・人員の確保（本調査 問 19）

(6) 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。「組織のトップ」とする回答が全体の 37.8%であった。

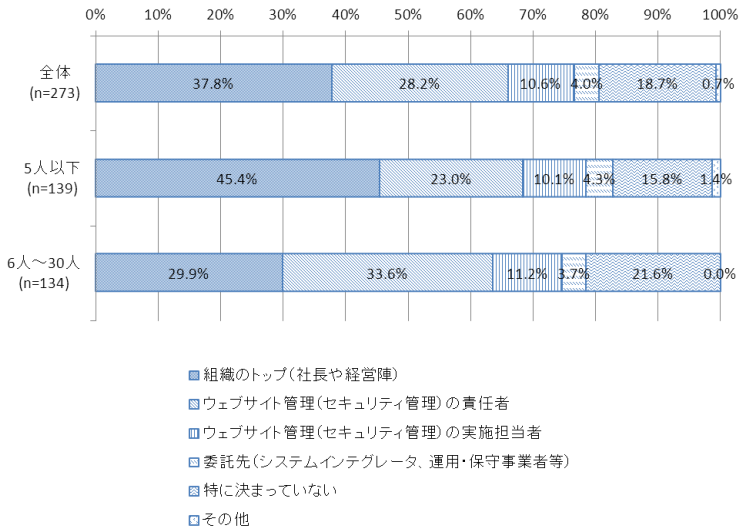

図 2.4.30 セキュリティ対策（脆弱性対策）に関する判断を行う人（本調査 問 16）

(7) 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。「ウェブサイト管理の実施担当者」とする回答が全体の 61.1%であった。

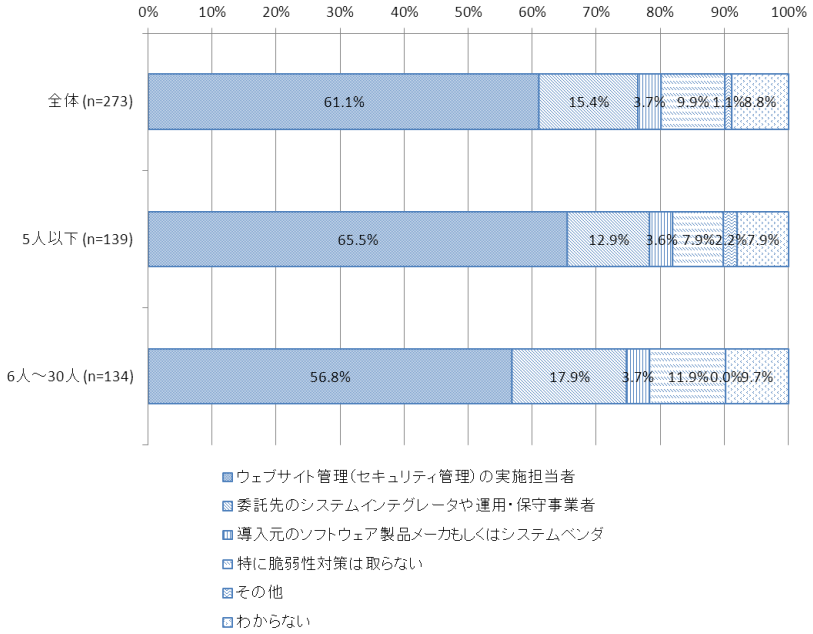

図 2.4.31 脆弱性対策を実際に行う人（本調査 問 18）

(8) 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尋ねた。課題としては「脆弱性やセキュリティに関する技術の習得が難しい」とする回答が多く、重要な課題としては「対策を行うための予算が確保できない」ことを挙げる回答が多かった。

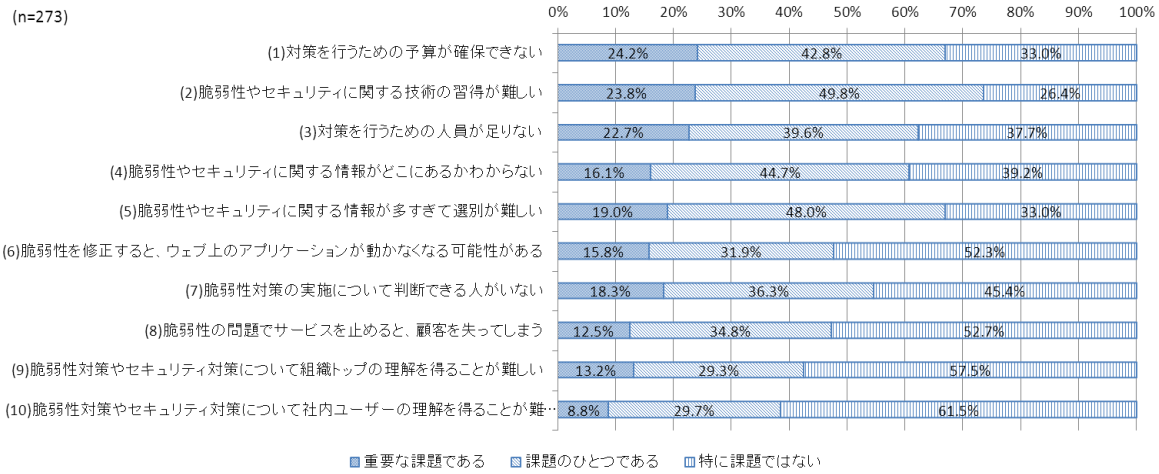

図 2.4.32 セキュリティ対策（脆弱性対策）の課題（本調査 問 20）

2.4.6. 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全体の約 4 割であった。

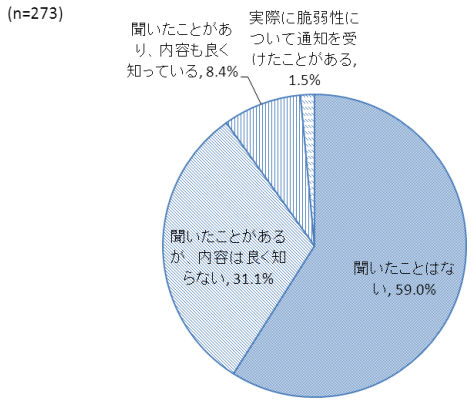

図 2.4.33 情報セキュリティ早期警戒パートナーシップの認知状況（本調査 問 21）

(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 36.2%）であった。

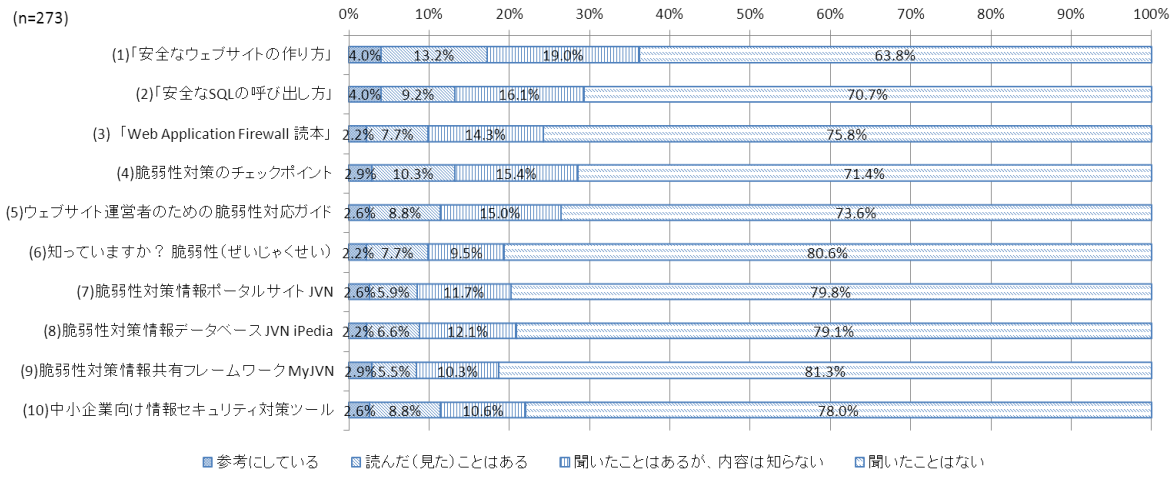

図 2.4.34 IPA による脆弱性関連の情報等の認知状況（本調査 問 22）

(3) 情報セキュリティ関連制度の認知状況

情報セキュリティ対策に関する代表的な制度について認知状況を尋ねた。「プライバシーマーク制度」は全体の約 7 割が知っており、「ISMS 適合性評価制度」「情報セキュリティ監査制度」は約 4 割の認知度であった。

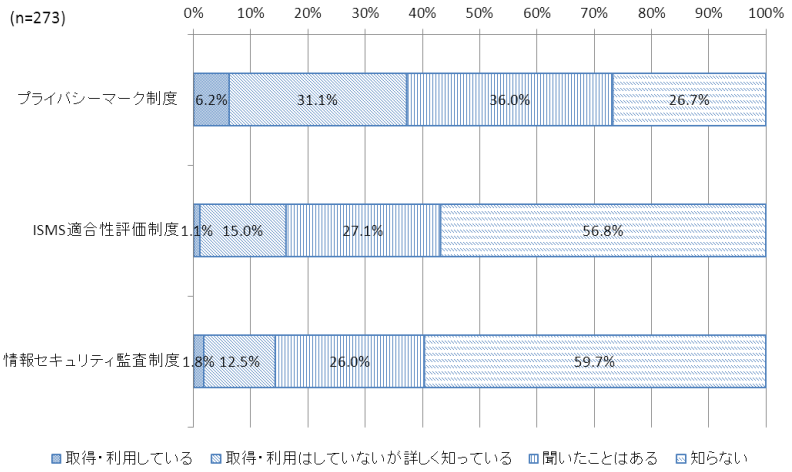

図 2.4.35 情報セキュリティ関連制度の認知状況（本調査 問 23）

(4) 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尋ねた（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」（42.1%）、「セキュアなウェブサイトの構築に関するコンテンツ」（38.5%）について比較的高い関心が示された。

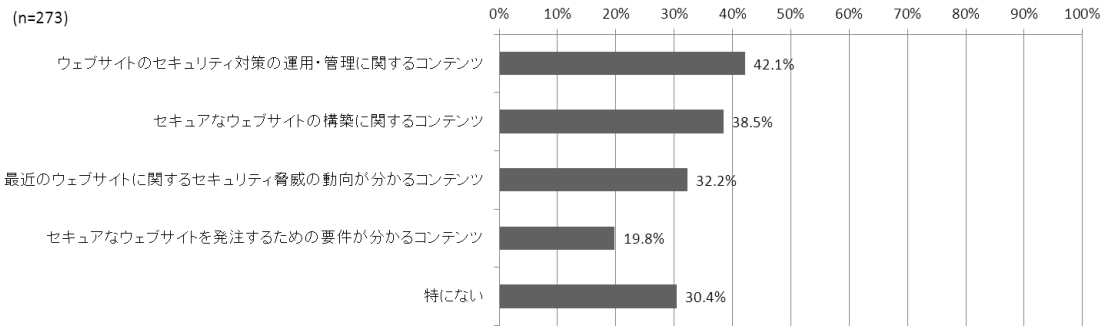

図 2.4.36 利用してみたい普及・啓発コンテンツ（本調査 問 24）

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 49.5%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 52.7%と多く、「担当者がいる」小企業は 21.6%、「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 16.5%にとどまった。(本調査 問 7)

これらの結果から、少人数でウェブサイトの運用をしている様子が裏付けられる。

(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 35.4%と多かった。この割合は従業員数 5 人以下の企業では 58.3%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 37.8%であった。(本調査 問 16)

これらの結果から、経営者がウェブサイトの構築および運用の方針に強く関わっている様子がうかがえる。

(仮説 3) セキュリティ対策は構築段階の対策が全てでその後は検討や改善は殆ど行っていない

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 45.4%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 19.0%であった。「構築時にのみ対策をしている」小企業は皆無（0.4%）であった。(本調査 問 12 および本調査 問 13)

これらから仮説は誤りであり、構築時の計画的な対策よりも運用時に必要に応じて対策が行わ

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 16.8%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 6 割は詳しく知っており、9 割は聞いたことがあるという結果を得た。（本調査 問 11）

一方で、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、「クレジットカード等の決済を行っていない」（59.8%）、「個人情報を扱っていない」（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」（33.3%）という理由を挙げる者が多かった。（本調査 問 14）

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」とする回答が半数を超えた。（本調査 問 20(6)(8)）

このことより、脆弱性の修正時に伴う問題についてまで深く考えて課題とする意識は必ずしも高くはない様子が伺える。

(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」（8.4%）、「おおむね確保できている」（35.6%）とする回答を合わせると約 4 割であった。一方、「やや不足している」（20.1%）、「まったく足りていない」（16.5%）とする回答も合わせて 4 割近くであった。「わからない」とする回答が 19.4%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 19）

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 6 割であった。（本調査 問 20(1)(3)）

従業員数が 6～30 人の企業においては、費用・人員が不足であるとする回答がより多かった。

(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（60.8%）、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 6）

「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 7 割であった。（本調査 問 20(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 4.8%、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 10.3%あった。これらを合わせ 15%の回答者が被害に遭ったと答えている。（本調査 問 17）

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 9.9%であった。（本調査 問 18）

(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 4 割であった。（本調査 問 21）

IPA による脆弱性関連の情報等の認知状況については、約 20～30%ほどが聞いたことがあるとしている。（本調査 問 22）

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 7 割であった。

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

	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 → 図 2.4.12 開発・構築の方法（本調査 問 1） → 図 2.4.16 経営層の関与（本調査 問 5）	・ホスティングを利用しコンテンツを自前で構築。 ・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。
ウェブサイトのセキュリティ対策（脆弱性対策） → 図 2.4.18 組織的なセキュリティ管理（本調査 問 7） → 図 2.4.30 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 16）	・経営トップが判断。 ・組織的にはあまり行っていない。	・ウェブサイト担当者（責任者）が判断。
セキュリティ対策の委託 → 図 2.4.19 外部委託の実施（本調査 問 8） → 図 2.4.20 セキュリティ要件（本調査 問 9） → 図 2.4.21 報告文書の取得（本調査 問 10）	・委託の実施率に差異はあまりない（わずかに低い）。 ・委託ルールが未整備（セキュリティ要件の指定、セキュリティ報告書の取得の割合は低い）。	・委託の実施率に差異はあまりない（わずかに高い）。 ・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セキュリティ報告書を取得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進めている小企業においては、対策を行っていない小企業に比べ、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（本調査 問 12 および問 13 を集約した結果）と組織的なセキュリティ管理の状況（本調査 問 7）についてクロスを取った結果を以下に示す。「構築時も運用時も脆弱性対策をしている」小企業においては、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 37.9%であった。一方で「一切脆弱性対策をしていない」とした小企業においてセキュリティ管理を「組織的には行っていない」企業は 89.2%にも及んだ。

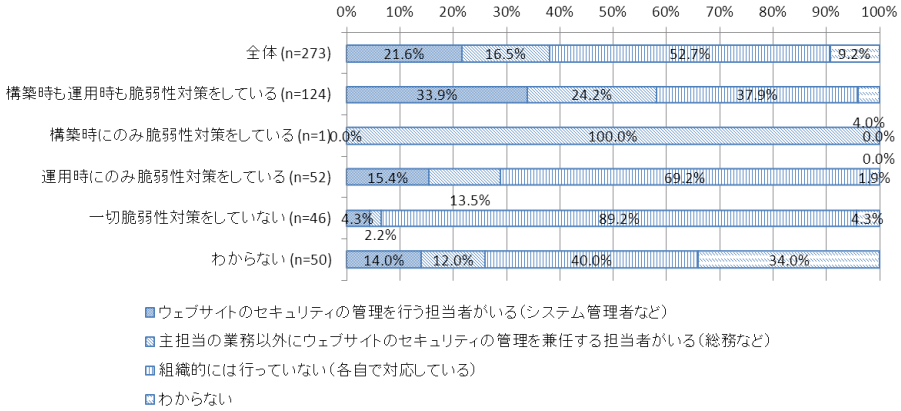

図 2.5.1 脆弱性対策状況 － 組織的セキュリティ管理の状況

脆弱性対策の状況（本調査 問 12 および問 13 を集約した結果）とセキュリティ対策（脆弱性対策）の判断を行う人の状況（本調査 問 16）についてクロスを取った結果を以下に示す。「構築時も運用時も脆弱性対策をしている」小企業においては、判断を行う人が「特に決まっていない」と回答した小企業は 8.9%であった。一方で「一切脆弱性対策をしていない」とした企業において判断する人が「特に決まっていない」と答えた小企業は 39.1%であった。

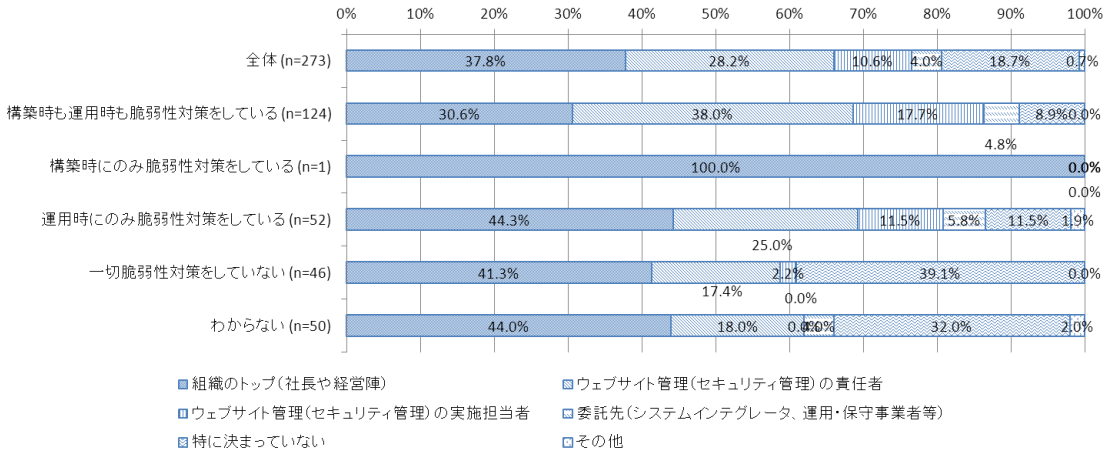

図 2.5.2 脆弱性対策状況 － セキュリティ対策の判断を行う人

3. 小企業のウェブサイトの運営者及び関係者に対するヒアリング調査

2 章の結果を踏まえ、脆弱性対策を促すための方策やその普及方策について、小企業のウェブサイト運営者や関係者にヒアリング調査を実施した。

3.1. 調査の概要

3.1.1. 小企業のウェブサイト運営者に対するヒアリング調査

小企業のウェブサイト運営者に対するヒアリング調査の概要を以下に示す。

［調査対象］小企業のウェブサイト運営者

（首都圏：5 件、地方中枢都市：3 件、地方中核都市：2 件）

アンケート調査回答者のうち、所在地とウェブサイトの形態から以下の対象者を抽出した。

表 3.1.1　ヒアリング調査対象者の属性

ウェブサイトの形態	首都圏	地方中枢都市*1	地方中核都市*2
オーサリングツール利用	3	1	2
独自開発	1		
外部事業者に委託		1	
ISP 提供サービス利用	1		
ショッピングモール利用		1*3	
合　計	5	3	2

*1) 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

*2) 地方中核都市：地方圏（三大都市圏以外の地域）における地方中枢都市以外の県庁所在地及び人口が概ね 30 万人以上の都市。

*3) 本回答者は、現状はショッピングモールを活用しているが、元々は独自開発をしていたことから、「独自開発」の意見や移行の意図等について確認するため、調査対象者に設定した。

［調査方法］ヒアリング調査

・首都圏（5 件）：グループインタビュー方式

・地　方（5 件）：訪問方式

［調査実施期間］2013 年 1 月

3.1.2. 業界団体関係者に対するヒアリング調査

小企業のウェブサイト構築・運用を支援する事業者等の業界団体に対するヒアリング調査の概要を以下に示す。

［調査対象］以下の 3 機関；

一般社団法人 日本コンピュータシステム販売店協会

一般社団法人 日本 Web ソリューションデザイン協会

特定非営利活動法人 IT コーディネータ協会

［調査方法］ヒアリング調査（訪問方式）
［調査実施期間］2013 年 1 月

3.2.調査項目

3.1.1、3.1.2 のそれぞれにおいて、以下の項目を中心に質問した。

・ウェブサイトの構築・運用の形態
・ウェブサイトの構築・運用のリソース
・脆弱性対策への課題
・脆弱性対策を促すための方策やその普及方策
・その他（アンケート結果に基づく確認点等）
※特に重要な知見はないため、記載は省略する

3.3.調査結果

表 3.3.1に調査結果を示す。また、その要点を以下に示す。

(1) ウェブサイトの構築・運用の形態

ウェブサイトの構築形態については、オーサリングツールを利用するケースが主流であった。使用するツールとしては、大半が「Dreamweaver」を挙げている。同製品を含め、オーサリングツールには、製品のコマンドを利用して生成したコードに脆弱性が含まれるケースやサンプルフォームに脆弱性が内包されているケースが指摘されている。したがって、使用するオーサリングツールのバージョンを最新に保つとともに、関連の脆弱性情報に留意することが望まれる。

また、ウェブサイトの運用形態については、多くがホスティングサービスを利用している。ホスティングサービスは、一般には OS やミドルウェアの脆弱性が発覚した際は、ホスティング事業者側がパッチ適用等の対策を実施する。そうした脆弱性対策の責任分担が明記されていることを確認すべきである。

(2) ウェブサイトの構築・運用のリソース

ヒアリング先の大半が、2 章の仮説検証で採り上げたとおり、構築・運用の担当を一人で任されている。任命は、スキルが評価されたわけではなく、「PC に慣れているから」「担当部門のメンバーだから」など、必然性の乏しい理由によるケースが多い。また、前任者の退職により、他に選択肢がなく、後を引き継ぐケースもある。これらの担当者にとって、サーバ等の IT 管理業務は既存の業務との兼務であり、負担となっている。担当者には問題意識や意欲もあり、可能であればセキュリティについて学びたいと考えているケースもあるが、学ぶ時間がないという指摘もあった。

ウェブサイトの構築は経営者が判断することが多いが、すべてに口を挟むわけではなく、詳細は担当者に任せている。一方で、ウェブサイトの運営に対する経営者の関心はあまり高くなく、たとえばトラブル対応に費用がかかることがわかると、「サイトそのものをやめてしまう」という

可能性も指摘されている。

(3) 脆弱性対策への課題

小企業において脆弱性対策が進まない理由の一つに、「自社のサイトは重要な情報がなく、著名でもないので狙われない」という思い込みが指摘されている。したがって、たとえ重要情報がなくても、脆弱性があるだけで狙われて踏み台にされてしまい、時に取引先にまで迷惑をかけるリスクがあることについて、理解していただく必要がある。

また、担当者にとっては、その脆弱性が自社に影響するのか、どのように対応すべきか判断できない状況があり、理解しやすい情報提供や専門家の助言が必要であるとの指摘もあった。

(4) 脆弱性対策を促すための方策やその普及方策

脆弱性対策を促す方策として、脆弱性の有無を検証するツールの提供が挙げられた。ただし、そうしたツールは攻撃を誘発する可能性もあり、提供方法に工夫が必要となる。

脆弱性対策を促す啓発資料を小企業に届ける手段として、商工会議所や関連業界団体との共同セミナーの開催、ウェブサイト構築やマーケティング等のイベントでのプレゼンテーション、関連業界団体の会員企業（システム販売店、ウェブ制作会社、IT コーディネータ）を介した情報提供等を展開することが提案された。

なお、首都圏と地方で、専門セミナーなど情報収集の機会の差は指摘されなかったが、首都圏では「システム構築事業者経由の提供」が有効との回答を得た一方、地方では「商工会議所のセミナー開催」が有効との回答が複数見られた。

表 3.3.1　ヒアリング調査結果とりまとめ

調査項目	首都圏（5 組織）	地方中枢都市（3 組織）	地方中核都市（2 組織）	関係者（3 組織）
(1) ウェブサイトの構築・運用の形態	・外部のストアツールを使っているため、今まではトラブルがなかったが、融通はきかない。将来的には CMS を使って全面的に書き換えたい。 ・主にコンテンツ制作を行っている。ウェブショップはやっていない。必要な情報を表示するページを担当している。 ・携帯向け動画サイトを扱っている。スマホのウイルス対策に追われている。運用は外部委託していて、パッチの適用を社外で行う場合もある。 ・顧客のウェブサイト構築は、コストや内容によってツール等を選択する。時間的制約もあって、使い慣れているツールを使ってしまう。規模が小さいと、セキュリティへの配慮が全くない場合もある。運用では、CMS やフレームワークに関して、簡単であればパッチを当てる。	・当初はネット販売のサイトを手作りで構築していたが、機能強化のため、外部のストアツールを活用してサイトを再構築した。 ・以前はウェブサイトを立ち上げ、運営管理を行っていた社員がいたが、退職したため、自分が会社に提案した。志願したわけではないが、必然的に担当になった。事業者に構築・運用を委託し、ホスティングを利用。社長は任せきりで、あまり興味がない。ビジネスにはあまり貢献していない。 ・顧客には、ホスティングのケースも、自社サーバのケースも両方ある。すでに顧客が持っている場合はそのサーバを利用する。	・顧客のウェブサイト構築では、データベースや動的なページは作らないようにしている。顧客には冒険は進めない。納品前にテストページで確認し、顧客と調整する。脆弱性がある場合、信用問題になると説明する。 ・バックアップとセキュリティの問題のため、顧客にはホスティングの利用を薦める。 ・小企業の経営者が自ら言うというより、通常は下からホームページ運営が提案される。声をあげた人が担当者となる。	・担当者１名が兼務で対応しているケースがほとんど。規模が大きくなるにつれて専任が増える。 ・アンケート結果は、リテラシーの高い層ではないか。 ・予算が無いので経営者が自分でやるしかないケースも多い。取引先の関係で、EDI などやらないといけない状況になると、社員にも振れないので、経営者が引き取る。 ・若い人が入ってきたから任せるという形が多い。地方では特にそうなる。 ・今までやっていた若い人がやめてしまうと放置状態になってしまうこともある。地元で運用している企業に運営を任せる場合もある。
(2) ウェブサイトの構築・運用のリソース	・ウェブサイトの作業は、全業務の 1 割以下であり、片手間で担当している。 ・ウェブサイト構築作業は、安く早くが求められる。セキュリティについては「うちには起こらない」と言われる。セキュリティは自己啓発のため勉強している程度。 ・今まで被害がなかったので、考えていなかった。セキュリティに重きは置いていない。コスト重視で、セキュリティは度外視だった。 ・費用対効果が重要だが、危機管理は別枠で考えるべきである。 ・経営者がセキュリティの重要性を認識しているので、予算や人手は十分にある。 ・相談できる技術情報を持っている人がおらず、ノウハウもない。勉強する時間もない。雑務に忙殺されている。外部委託も検討したい。 ・脆弱性のチェックツールを提供してほしい。 ・現状は問題がある。まずは自分が技術的に詳しくなりたい。	・消去法で指名されて、モール担当になった。構築は独学でやった。中国からメールを受け取る際には感染を避けるため、専用の PC を使っている。顧客情報は、サイトには置かない。6-7 万円／月で運用を代行するという売込みがあるが、業務範囲はアバウトである。 ・担当は自分一人のみ。セキュリティ対策も含め、IT 関係全般担当である。セキュリティに関する知識は技術研修の中で知ったが、脆弱性のリスク認識は十分でない。サイト運用は外部委託で、他の仕事と兼任で対応している。大半は他の仕事。構築、運用時に脆弱性対策は気にしていない。ウェブ上の機能が乏しく、機微情報を扱っているわけでもない。改ざんされても別に特に問題ない。業者からセキュリティの話は出ていない。 ・クロスサイトスクリプティング、SQL インジェクションを防止することは必須。また、入力に関しては非常に注意を有する。「全くわかっていない」、「初めて」という人が多く、運用まで指導しないと構築しても回らない。	・セキュリティ関連の作業は全体の 1 割程度。一般の人に対する技術の翻訳者となっている。セキュリティに関しては、顧客の上司を説得する役割も担っている。知り合いの同業者間で、お互いに制作したウェブサイトのクロスチェックを行う。商工会や商工会議所に相談はあるが、どこに話を回してよいかわからないらしい。 ・リスクを考えて Java は使わない。プログラムに関しては、しっかりした業者に相談して作成する。フリーだと、安かろう悪かろうになる。それらを前提として提案し、cgi を作成する。脆弱性対策を実施するかどうかの決断は、担当のみでは決められず、経営者が決めるしかない（「わかりました、相談します」となる）。	・脆弱性について聞いたことがあるという人は多いだろう。しかし、脆弱性の情報収集やパッチあてをやっているかどうかは、わからない。 ・最低限これをやっておいたほうがいいということをユーザも欲しいと考えている。ユーザは情報を持っているが、自分のシステムにどう適用できるかは判断がつかない。販売店の人が積極的にやってくれるとうまくいくように思う。 ・サーバにパッチをあてるのは一般には無理だろう。業界でもサーバをいじれる人間は専門家。利用者は気にしていない。作り手側が調べることも多い。 ・外部に出そうという考えが増えている。移行期にある。自社で何百万もかけていたが、レンタルサーバに変えたいという意見はある。
(3) 脆弱性対策への課題	・経営者はセキュリティに関して話は聞いてくれるが、深刻さはわかっていない。 ・重要な情報を扱っていないので、脆弱性対策はしていない。ショッピングは別のサイトを使うため、大掛かりなセキュリティ対策は必要ない。 ・現状では気にしていないという回答をしたが、ある程度の対応はすべきであると考えている。 ・セキュリティに力は入れていない。個人的には多少は考慮したい。 ・パッチを当てるか否かはシステムおよび業務への影響度による、ケースバイケース。都度調べる。 ・踏み台になることは恐い。	・構築の段階で脆弱性対策を心がけるようにすべきだが、要件がわからない。全てを気にかけると業務が遅延する。担当に任せっきりで、トラブルが発生してから対応する。ホームページは、他社から自社を認知・認証するための基本なので、改ざんされてはならないが、チェックできていない。脆弱性があった場合何をすればよいかはわからない。何が危険かよくわかっていない。 ・自社ではセキュリティ対策自体が不要と考えている。ウェブサイトを止めると顧客を失うことが問題。セキュリティの話でかつコストの上積みがあったら、社長判断となる。社長はウェブサイト	・小企業の担当は、セキュリティに詳しくないことが多い。報道されると社長から電話がかかってくることも多い。説得の際は、信用を失うなど、痛い目に合った話をする。重要な情報がない場合でも、踏み台になるリスクを強調する。踏み台やスパムメールの発信元になるという話は、説得性がある。社長が必要性を認識すれば後はすんなり行くことが多い ・「緊急」と言われても、どこまで対応すべきか不明。アウトソーシング先のサーバの脆弱性をチェックする術がない。詳しい人に相談できる環境が非常に重要。今目の前にある不具合をどう直せ	・ファイアウォールやウイルス対策をやっているから大丈夫と思っているのが実態。侵入される事態は、自分のところでは起きないと思っている。 ・ウェブサイトには社長が関わっているが、彼らが理解しないとお金が出ないので対策には動けない。根本のところの理解が足りていない。脆弱性とウイルス感染の区別がつかない。 ・ウイルス対策をしているからうちは大丈夫だろうという安心感がある。被害に遭う実感がない。起きない事故に備えるのはお金の無駄と考えている。 ・どうしてもサイトを持たなければならないとい

調査項目	首都圏（5 組織）	地方中枢都市（3 組織）	地方中核都市（2 組織）	関係者（3 組織）
	・クライアントの意向はあるが、独断で止めてパッチを当てる。止めて文句を言うクライアントはいない。 ・脆弱性が見つかったら、措置すべき。携帯向けであり、個人情報を扱っているので最優先対応が必要。利益が減ってもやるべき。 ・導入が容易なマニュアル等があれば、導入したい。IPA で用意できないか。技術的に難しい。	維持にはこだわりがなくやめることもありうる。 ・少人数の会社の場合、セキュリティに詳しい人はいない。顧客からセキュリティの要求がされることは無い。顧客におけるセキュリティ確保の課題としては、「予算確保」「技術の習得が困難」「人員不足」「情報の所在が不明」が挙げられる。 ・対策に関して判断できる人がいない。自分は関係ないと思っている人も多い。	ばよいか教えてほしい。 ・担当は決まっていても、勉強できる時間がない。 ・「自分は被害者にならない」からやらないという意識。他人に迷惑をかけると説得するとよい。そのリスクをお客さんに知ってもらう。 ・担当者には、どこが危なくてセキュリティが必要なのかわからない。専門用語もわからない。意識を変えるしかない。	う必要性がなければ切り捨てられる。問題だったらやめてしまえばいいと思っている。 ・踏み台にされるケースの問題についてニュースで報道されても、何がまずいか理解できない。当事者意識はない。顧客や取引先に言われるとやらなくてはと考えるように変わられる。そのあたりからスタートしてはどうか。
(4) 脆弱性対策を促すための方策やその普及方策	・セキュリティには必要以上に気を配ったことはない。乗っ取り等の話は聞くので、勉強したい。 ・現場の技術者向けのコンテンツが欲しい。経営者にも転用可能。 ・情報セキュリティのポータルサイトが欲しい。経営者向けは損得勘定の視点が重要。 ・経営者向けと技術者向けの両方がほしい。経営者向けは専門的な部分に踏み込まないで被害の実態を訴えるもの。 ・攻撃スクリプトを IPA から送ってもらって、実演できると良い。 ・経営者はサービスとして認識すべきである。技術者向けは、情報セキュリティの駆け込み寺として機能するとよい。 ・クライアントは知識ゼロの場合が多く、そうした場合、コストも負担してくれない。実際に目で見えると、クライアントに説明できる。 ・Youtube での配信は有難い。ポータルサイトがよい。Twitter や Facebook も使ってほしい。 ・導入事例で、費用も明示して頂きたい。予算との関係を明示する。低予算でもこれぐらいできるだろうという事例があるとよい。 ・セキュリティ情報を顧客に持ち込むのに適しているのは、システム構築事業者ではないか。Web デザイナは追いついていない。 ・デザイナがよいのではないか。他の人は話が難しい。	・こんな事例があったということをわかりやすく示して、危険性を表現してほしい。 ・内容が堅いと、免許の更新のガイドブックのように読まれない。言葉はわかるが頭に入らない。 ・LINE で宣伝すればよいのではないか。 ・フローチャートで示してはどうか。 ・連絡先情報は重要。 ・定期検診のサービスを行うサイトがあるとよい。「最近検査していない」という連絡をするようにしてはどうか。 ・Youtube ビデオは興味深い。画像で「こうなる」ということがわかるとよい。 ・オンラインでウイルスチェックするように、脆弱性をチェックできるとよい。 ・ホスティング会社と提携して、脆弱性の対策を行ってもらってはどうか。また、SSL 認証ベンダと提携して、コンテンツとしてリンクを貼ってもらう形はどうか。 ・ウェブサイト構築に際し、セキュリティを学ぶ機会はほとんどない。ウェブ構築関連・マーケティングに関するイベントで話をしてはどうか。	・脆弱性に関してはネットで検索するので、サーチエンジン上位に出てくることが必須。 ・セミナー開催も有効。商工会議所でセミナーを行うとよい。商工会議所や青色申告会との連携も重要。建築業者向け業界団体などもよい。商業高校での授業も重要。 ・IPA が簡易評価認証制度を行う。たとえば電子入札の際、IPA の認証マークを貼り付ける。 ・セキュリティ情報は、興味ある人しか見ない。まず、セキュリティに興味を持ってもらうことが重要。 ・簡素にまとめられたパンフレットが必要。文字ばかりでは興味を持ってもらえない。 ・ホームページ構築に際しては、商工会や商工会議所に相談するので、IPA も商工会や商工会議所と連携すべき。	・「脆弱性」という表現が難しい。「セキュリティ上の弱点」がよいのではないか。 ・会員が有効活用するようにする。サンプルを配布してもらい、追加要請があれば使われていると分かる。ドアオープナーとして使えるとよい。 ・販売店が自分で印刷して持っていくか。印刷物をいただければ、販売店に配ってみてくれと渡すことはできる。 ・HTML チェッカーのように脆弱性チェッカーのプログラムが欲しい。公的な団体から提供していただけると助かる。作り手としても、セキュリティ対策を適切に実施するほうが正しいので、文句は言い難い。 ・Web ディレクターの検定で必須の項目にできる。テキストにも書けるだろう。 ・構築後に運用費をもらえることはほとんどない。手間をかけずにチェックできれば助かる。 ・Web ディレクターが必要性を知っているかが分かれ目。ディレクターが顧客と話して要件定義をしていくので、詳しくないと困る。Web ディレクターにトラブル事例や具体的にどんなプログラムや管理が問題であったかを示すことは有効。 ・自社サーバでウェブアプリを作って XSS 脆弱性が発生するようなケースと、マネージドサーバのケースでは対策の方針が異なる。 ・「脆弱性をチェックしてください」と書いた場合、専門知識が無いので、噛み砕いて伝えないとわからない。専門家に任せるのが良い。 ・対策のポイントについては、「こんなこともしましょう」ではなく、「これをやりましょう」と言っていただいた方がいい。 ・専門的な言葉は一切使わない方がいい。XSS みたいな言葉はいっさい説明もしない方がいい。 ・セキュリティ事業者は高い。小企業向けに安くやってくれるところはあるか。 ・IPA のコンテンツは豊富だが、経営者が見に行くかにはハードルが高い。入口はいくつかあると思う。付き合いのあるところから情報が入ってくれば探すだろう。 ・やらなければいけないと思っていただくところまでできるが、どうしたらいいかの最初の一歩が

調査項目	首都圏（5 組織）	地方中枢都市（3 組織）	地方中核都市（2 組織）	関係者（3 組織）
				踏み出しにくい。強制的に圧力、外圧がかかれば、一番効果がある。 ・IT コーディネータの方に資料について知っていただくことは可能。ML で流すこともできる。 ・相談相手として、地元の IT コーディネータを活用するという流れであれば、活性化につながる。