地方公共団体における脆弱性対策の実態に関する調査報告書

2012 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

地方公共団体はインターネットを通じて不特定多数のユーザにサービスを提供しているが、そのサービスが稼働するシステムにおいて脆弱性が存在する場合がある。

脆弱性は悪意ある者からの攻撃の的であり、その脆弱性情報は外部に漏れぬように適切に管理し、情報を基に早急に対策をとることが求められる。しかし地方公共団体は、地域住民に対し情報を公表しないことは問題であるという考え方があり、これにのっとると脆弱性対策が十分でない状況のなか、脆弱性を公表しなければならず、結果的にサービスを利用しているユーザ全体を危険な状況に陥れることになる。

このような背景の下、本調査では、地方公共団体と脆弱性情報を共有する現実的な方式の特定を目的とする。

1.2. 調査対象

■地方公共団体に対するアンケート調査

地方公共団体を対象とするアンケート調査を実施し、脆弱性対策の実態や公表のあり方に関する考え方や問題点を調査した。

［調査方法］郵送アンケート調査

［調査対象］地方公共団体（情報セキュリティ部署）

47 都道府県、23 特別区、786 市 [1]

［有効回収数］399 件 (47.6%)

■地方公共団体関係者に対するヒアリング調査

地方公共団体関係者から脆弱性対策及びパートナーシップに関する理解を促すための方策についてヒアリング調査を行った。

調査は、アンケート調査回答課の職員を対象に 8 件実施した。

［調査方法］ヒアリング調査

［調査対象］アンケート調査回答者のうち、次のいずれかのケースに該当する方を対象とした。

- 脆弱性対策を複数実施しているケース
- 脆弱性対策を複数実施していないケース
- 脆弱性情報の公表について自治体の方針と合わないケース

[1]全国市長会に登録のある市(平成 23 年 11 月 11 日現在)を対象とした。ただし、東日本大震災で大きな被害を受けた岩手、宮城、福島３県の沿岸部を除く。

1.3.調査実施期間

2011 年 9 月～12 月

1.4. 調査項目

調査の主な設問項目は以下の通りである。

＜アンケート調査の設問項目＞

1. 地方公共団体の規模、ICT 環境
2. 脆弱性関連情報の収集に関する実態
3. 脆弱性対策の実態
4. 脆弱性情報の公表に関する理解
5. 脆弱性対策や脆弱性情報の公表に関する問題点
6. 情報セキュリティ早期警戒パートナーシップに関する認知度

＜ヒアリング調査の設問項目＞

1. 情報システムの脆弱性問題に関する方針
2. 情報システムの構築・運用時の脆弱性対策の慣習
3. 情報公開ポリシーとの関係（透明性と公表によるリスクのバランス）
4. 脆弱性対策について啓発が必要な層とその内容
5. 策定する啓発資料の配布方法（効果的な普及策）に関するご意見

1.5.調査結果概要

1.5.1.情報公開ポリシーと脆弱性情報の関係（透明性、安全性、可用性のバランスについて）

・ 運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応として、『1.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知するが、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ。』は 5.0%が選択した。この場合、対策が適用される前に公表すると、システムが攻撃され住民の情報が流出するなどの被害が生じるリスクや他組織の類似システムが攻撃対象となるリスクがあるが、回答者がそれらのリスクを認識していない可能性がある。また、『2.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知し、当該システムを安全のため対策完了までは停止する』については、35.1%が選択した。この場合、他組織の類似システムが攻撃対象となるリスクがあるが、回答者がそのリスクを認識していない可能性がある。（アンケートより、4.1節参照）

・ 「公開が行政のあり方である」という意見もあり、未公表の脆弱性でも公開される可能性がある。その一方、「未公表の脆弱性情報は『公開により住民に被害の及ぶ可能性がある場合は非公開にして良い』という例外条項に該当する」という意見もある。また、サービスを停止する場合は、住民や議会に説明を求められることもある。（ヒアリングより、3.4.1小節参照）

1.5.2.啓発対象と内容、および効果的な普及策について

・　啓発対象と内容について、下表の通りの意見を頂いた。

啓発対象	主な意見
経営層・予算管理層	・被害事例における被害額を地方公共団体の予算と関連づけて示す。 ・脆弱性の対策を怠って被害が発生した場合、結果的に市民からの信頼を失う恐れがあることを示す。 ・テレビや新聞で報道されている事例について示す。 ・統計情報を継続的に提示する（例：周辺都市におけるツールの導入状況）
オーナー部門（原課）	・原課における脆弱性対策の方法について示す。 ・IT 担当部門による支援の必要性について、マニュアル・ガイドラインの形で示す。 ・委託先への注意喚起も重要であるということを示す。
IT 担当部門	・IT 担当部門が脆弱性の情報をうまく裁けるような体制管理に関する資料を示す。 ・どういう手法で、どこが狙われているかといった差し迫った情報を示す。

・　また、効率的な普及策として、啓発資料の配布を『都道府県により開催される地域の勉強会』にて配布する、IT 担当課に直接送付する、LASDEC のメーリングリストからお知らせとして送付する、などの意見を頂いた。（ヒアリングより、3.4.2小節）

1.5.3.「脆弱性情報に関する透明性、安全性、可用性の判断」に対する「情報セキュリティ早期警戒パートナーシップに対する認識」の影響

・　パートナーシップから脆弱性の通知を受けたことがある組織の 43.8%が『攻撃を受けるリスクを抑えるために脆弱性の存在については対策を適用するまで住民への公表を控え、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ』としており、より客観的に脆弱性のリスクやサービス維持の必要性を判断したと考えられる。しかし、同パートナーシップは、8 割近くの地方公共団体からは十分に認識されておらず、同パートナーシップの普及啓発を継続することが求められる。特に、人口の少ない市における認識度が低いため、重点的な対策が求められる。（アンケートより、4.1.2小節参照）

2.調査分析の方針

2.1.調査仮説

次の調査仮説を立てて調査にあたった。

- 地方公共団体が入手する脆弱性関連情報はLASDECからの配信と出入りのSIerからの通知が主。
- パートナーシップに関する認知度は高くない。
- 脆弱性対策はSIerの示す対応計画を許可する形が多い。
- 入手した脆弱性情報は、即座に地域住民に公表すべきと考える自治体も見られる。
- 自治体にとって、未公表の脆弱性情報を知りながら公表しないリスクと、公表により危険性が高まるリスクをどのように理解するかが問題となる。
- 脆弱性対策の阻害要因

  （阻害要因の例）

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

2.2.アンケート調査結果の取りまとめ方針

回答者の所属する企業規模については、都道府県、特別区、市で分類した。また、人口区分による分類も行った。

2.3.ヒアリング調査結果の取りまとめ方針

ヒアリング調査結果は、以下の3つの観点で取りまとめた。

1. 地方公共団体と脆弱性情報を共有する方式を探る上で重要な、情報公開ポリシー(透明性)と公表によるリスクのバランスについて地方公共団体のとらえ方を整理する。
2. 1のとらえ方の背景となる、情報システムの構築・運用時の脆弱性対策の慣習について整理する。
3. 地方公共団体に対して脆弱性対策を啓発する際に、提供対象とするべき層とその内容、および効果的な普及策に関して整理する。

3. 調査結果

3.1. アンケート回答地方公共団体の概要

3.1.1. 都道府県、特別区、政令指定都市からの回答状況

表 3.1-1に示す通り、いずれも 50%程度に達する高い回収率であった。

表 3.1-1　都道府県、特別区、政令指定都市からの回答状況

都道府県庁 の合計	特別区 の合計	政令指定都市 の合計
24 (51%)[2]	11 (48%)	8 (42%)

3.1.2. 市からの回答状況

表 3.1-2に示す通り、市からも 46%という高い回収率であった。

表 3.1-2　市からの回答状況

市 の合計（政令市含む）
358 (46%)

人口別の回答状況は図 3.1-1の通り。

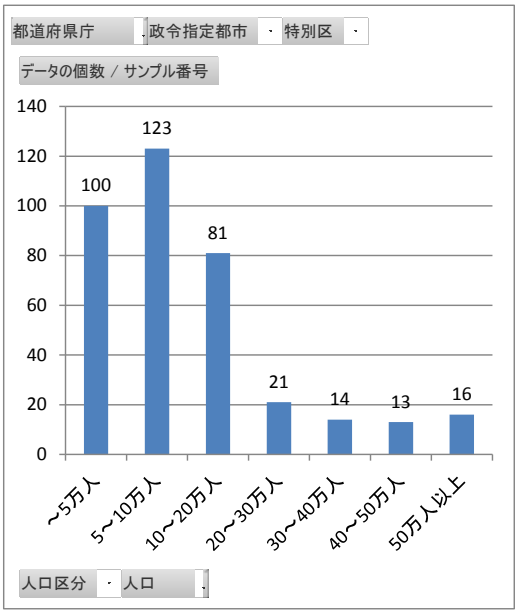

図 3.1-1　人口別の回答状況

[2] 回収件数。括弧内は回収率

3.2.アンケート回答の概要

3.2.1.直近 1 年間にかけた IT 関連の支出の総額(概算)について

都道府県、特別区は直近 1 年間にかけた IT 関連の支出総額が 10 億円を超えることもそれぞれ 62.5%、63.6%と多い。市は 10 億円を超えることは 11.2%と比較的少ない(図 3.2-1)。

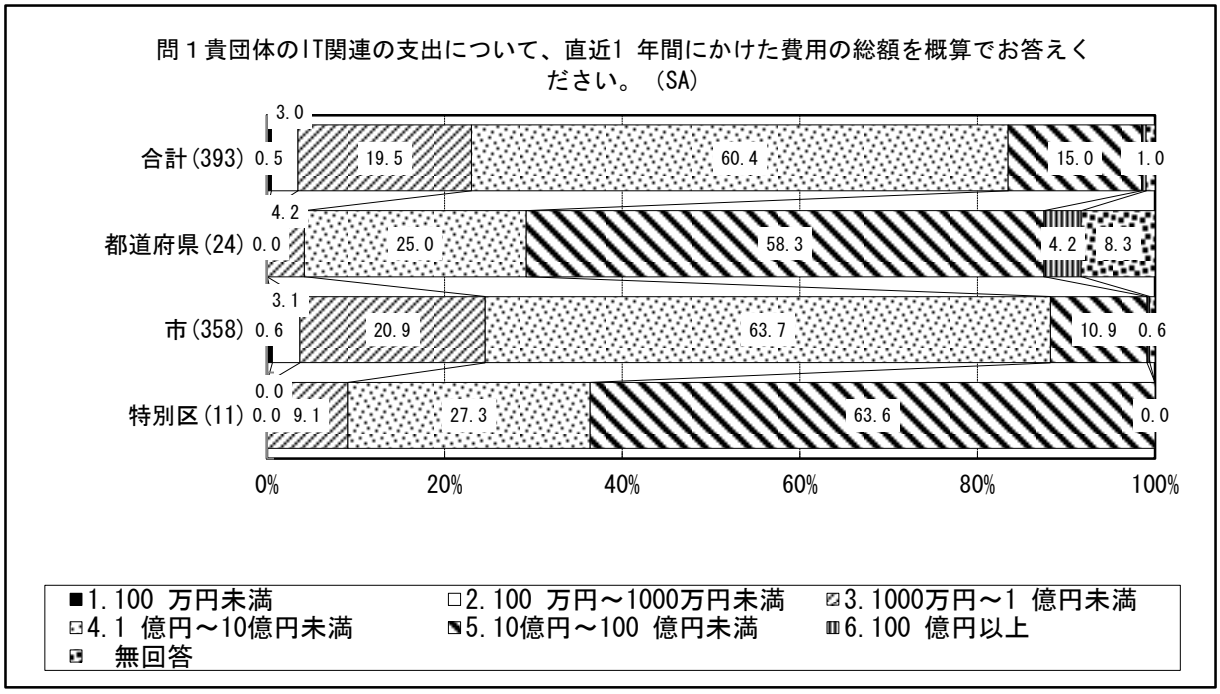

図 3.2-1 IT 関連の支出[3]

[3]図中の設問部に記された「(SA)」は、アンケートの質問が、単一回答方式であることを示す。

3.2.2.直近 1 年間に情報セキュリティにかけた支出の総額が IT 関連支出に占める割合について

IT 関連支出のうち、情報セキュリティにかけた支出の総額が占める割合は 5%以下である地方公共団体が合計 66.7%と多い。都道府県は「7.わからない」という回答が 62.5%を占めた。

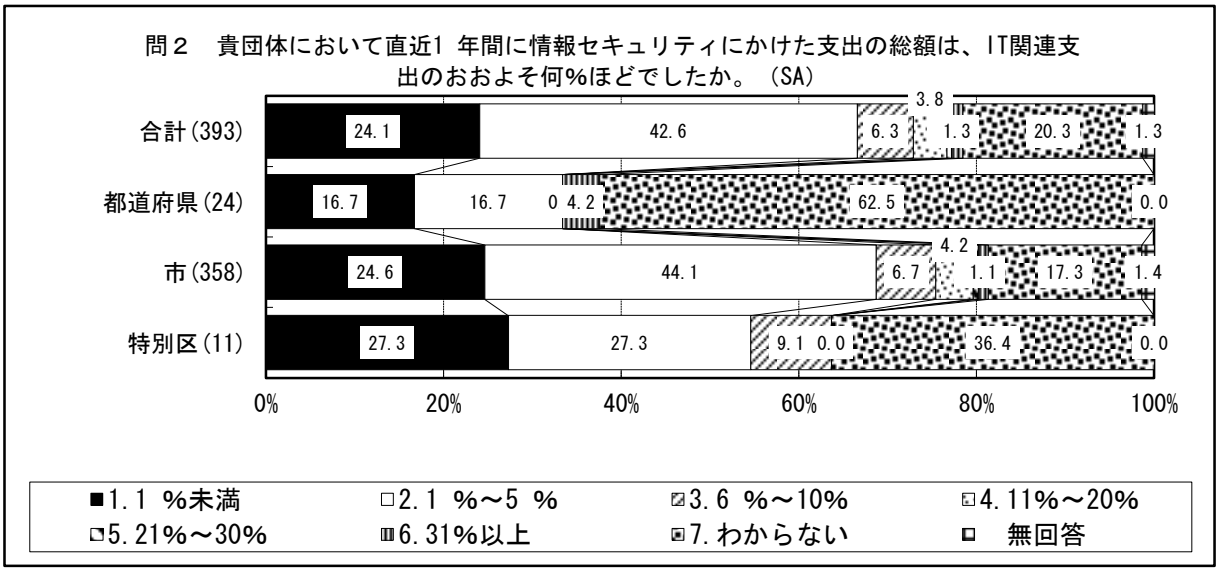

図 3.2-2　情報セキュリティ関連支出の IT 関連支出に占める割合

3.2.3.現在のウェブサイト関連システムの導入状況について

都道府県、特別区、市とも、『a.住民・企業向けホームページ』については99%以上で稼働中であった。都道府県、特別区については、『b.電子申請システム』『c.電子調達システム』『d.電子申告システム』『e.電子収納システム』など、市よりも稼働中の割合が高い。特別区では、『h.電子予約システム』『i.証明書発行システム』の導入が進んでいる。

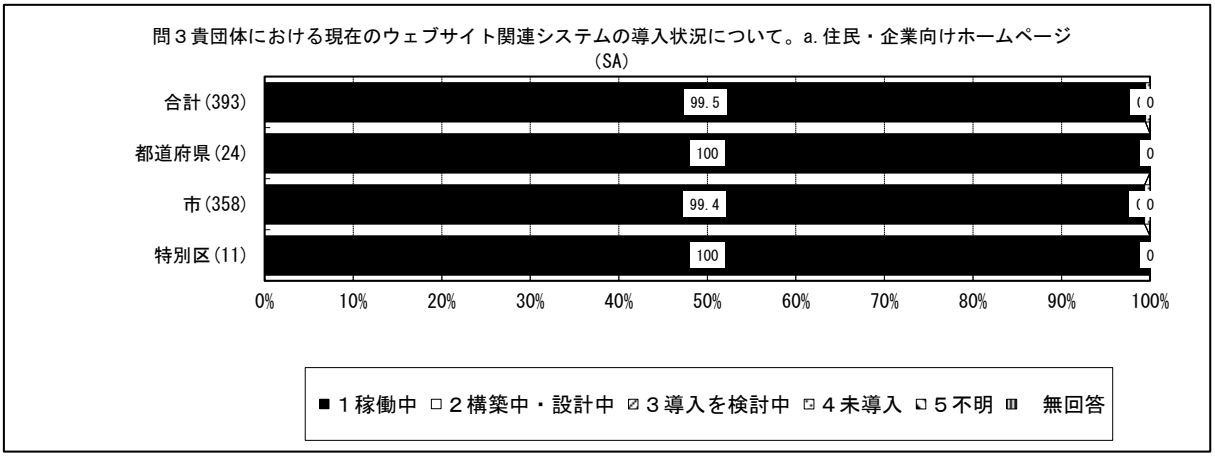

図 3.2-3　導入状況（a.住民・企業向けホームページ）

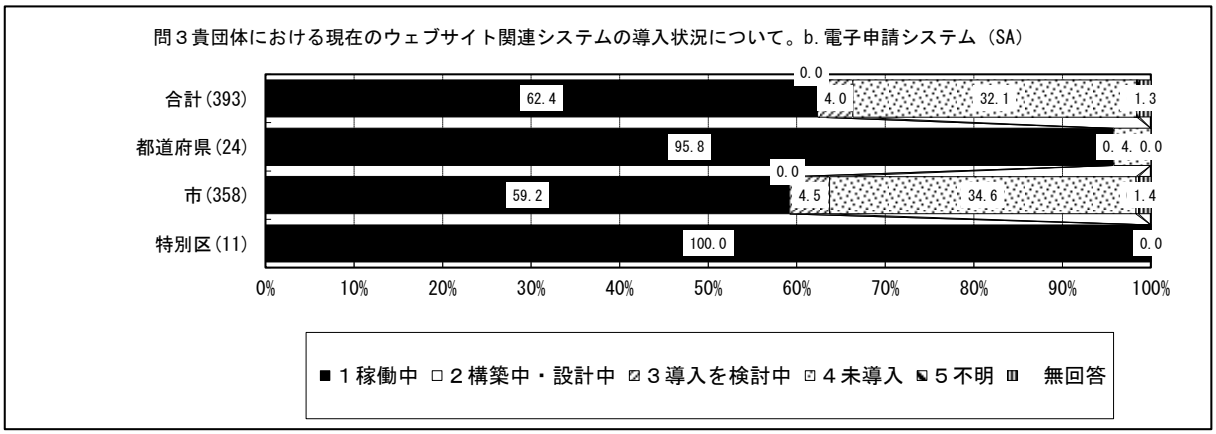

図 3.2-4　導入状況（b.電子申請システム）

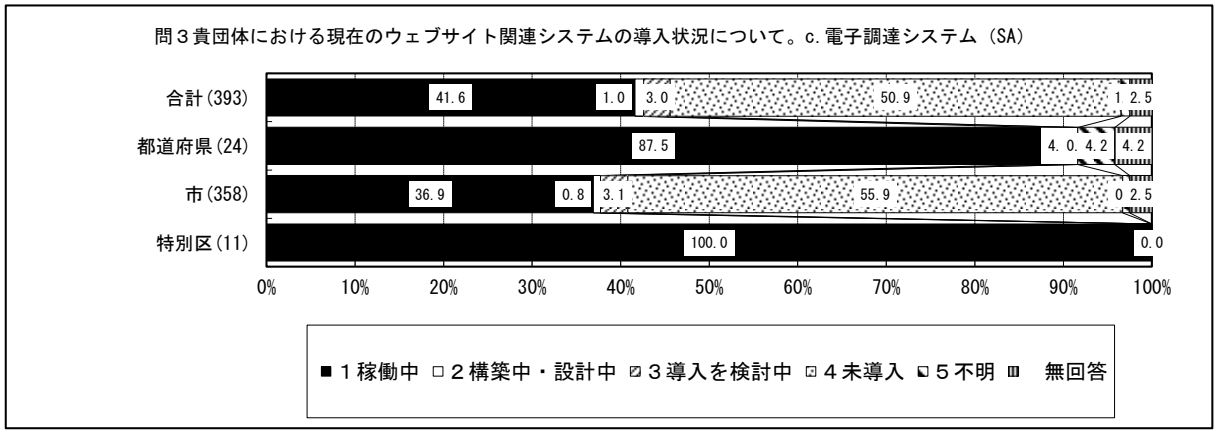

図 3.2-5　導入状況(c.電子調達システム)

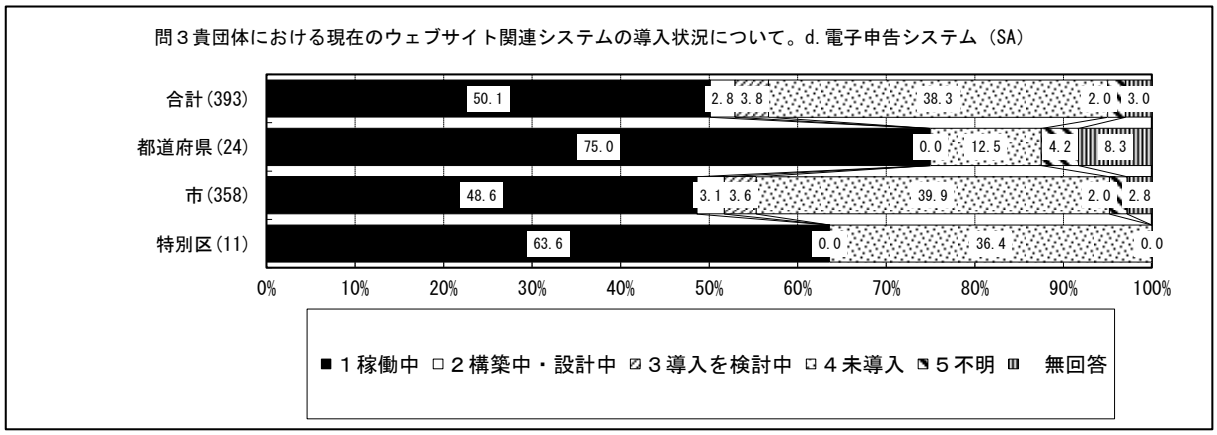

図 3.2-6　導入状況(d.電子申告システム)

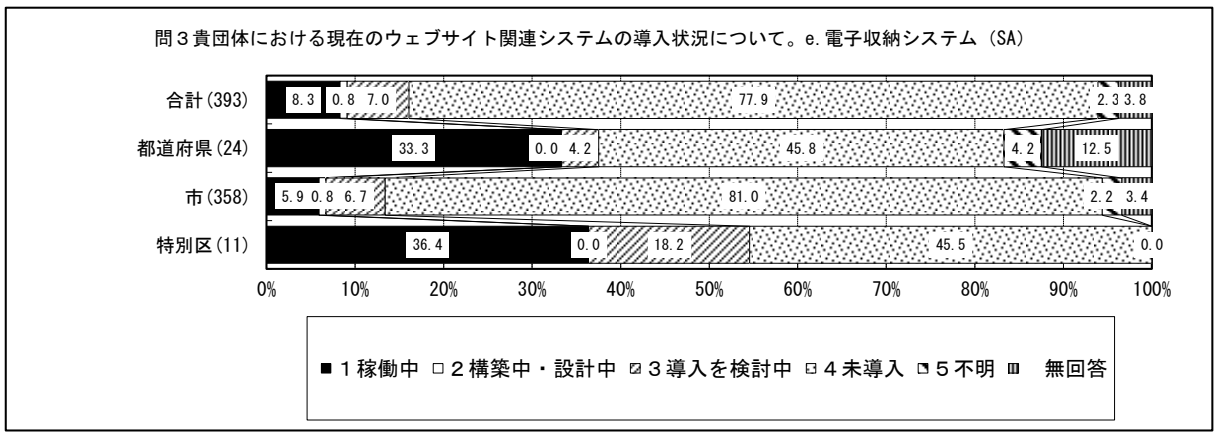

図 3.2-7　導入状況(e.電子収納システム)

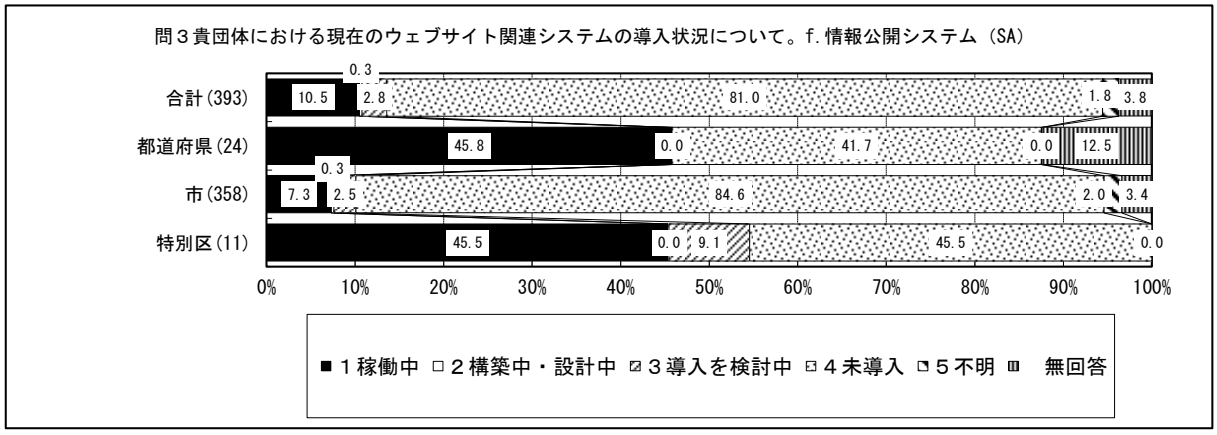

図 3.2-8　導入状況(f.情報公開システム)

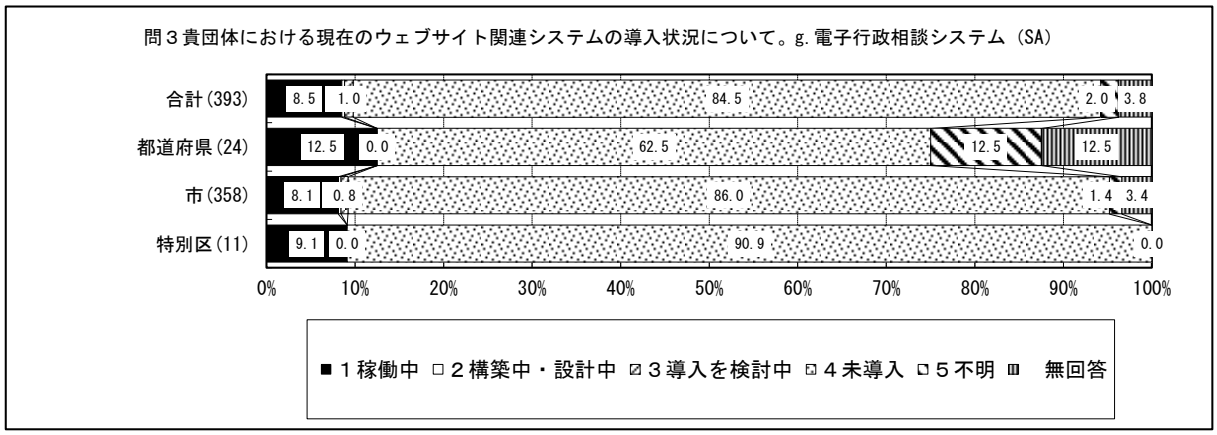

図 3.2-9　導入状況(g.電子行政相談システム)

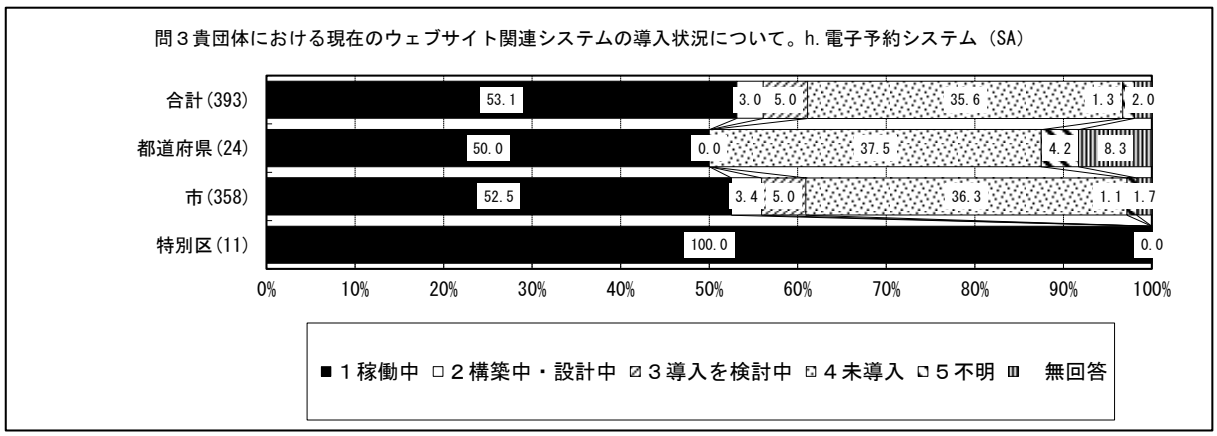

図 3.2-10　導入状況(h.電子予約システム)

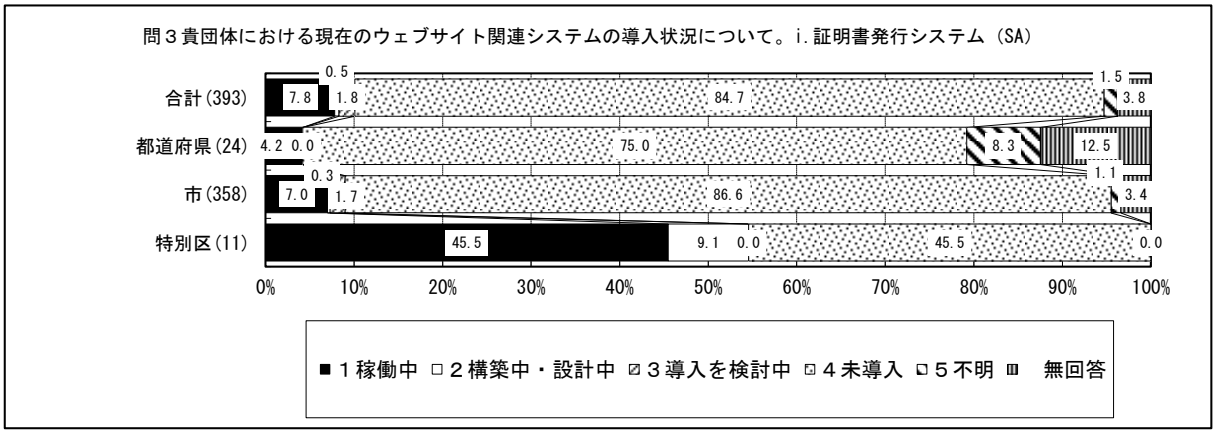

図 3.2-11　導入状況(i.証明書発行システム)

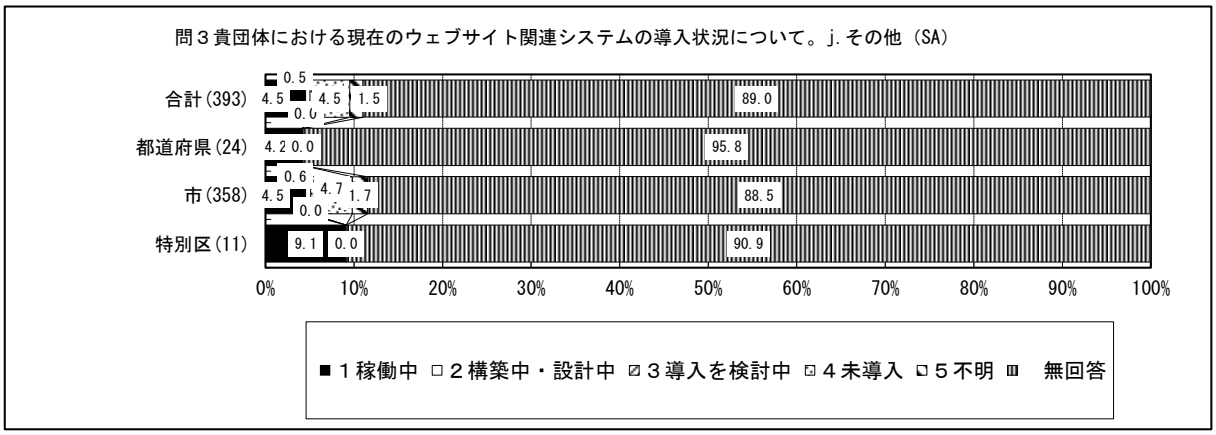

図 3.2-12　導入状況(j.その他)

3.2.4. システムの運用・管理の主体について

［ 3.2.3 で「1.稼働中」「2.構築中」のいずれかに○印をつけたシステムについて］

民・企業向けホームページの運用・管理は、市の場合、職員が担当する割合が 73.3%と高く、都道府県の場合、外部事業者に委託している割合が 79.2%と高い。

また、『b.電子申請システム』『c.電子調達システム』『d.電子申告システム』については、共同利用システムを利用する割合が多い。

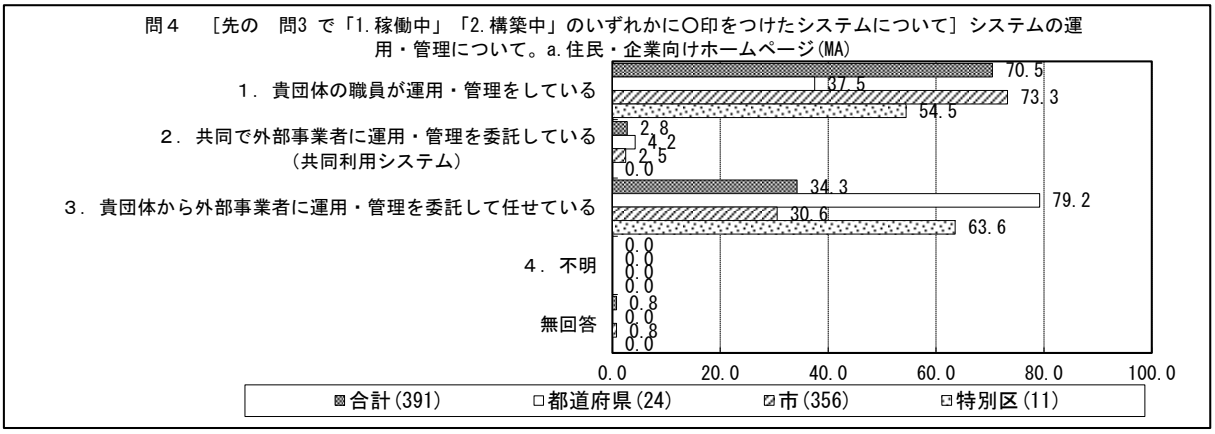

図 3.2-13　システムの運用・管理の主体について(a.住民・企業向けホームページ)[4]

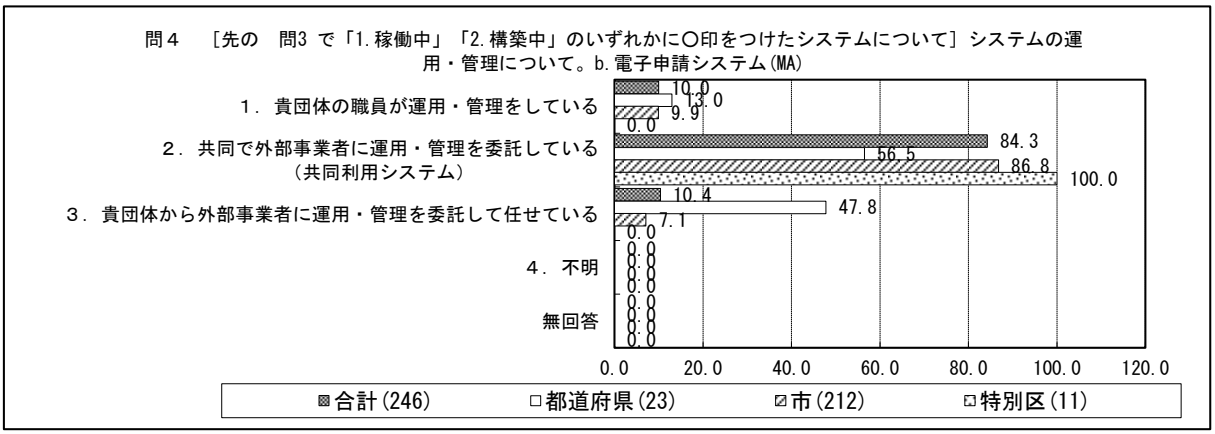

図 3.2-14　システムの運用・管理の主体について(b.電子申請システム)

[4]図中の設問部に記された「(MA)」は、アンケートの質問が、複数回答方式であることを示す。

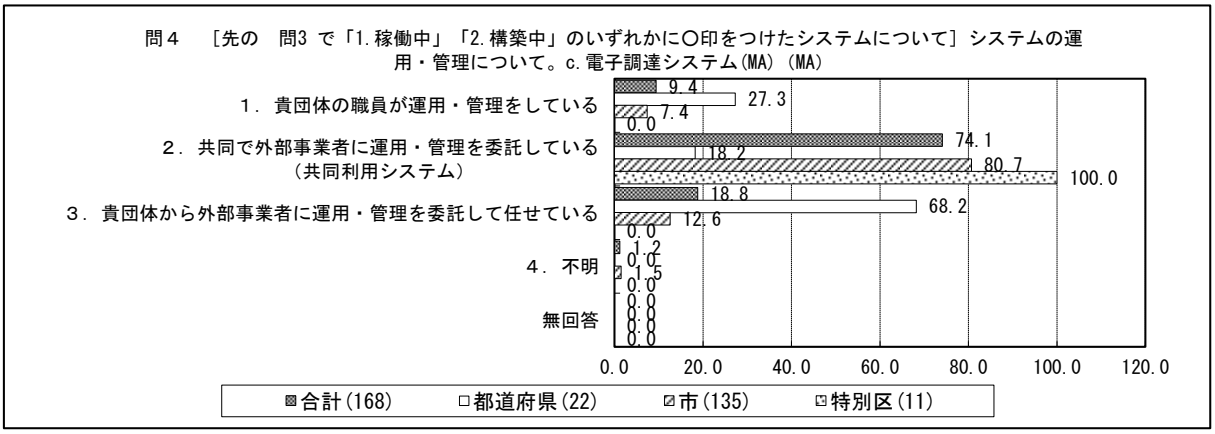

図 3.2-15 システムの運用・管理の主体について(c.電子調達システム)

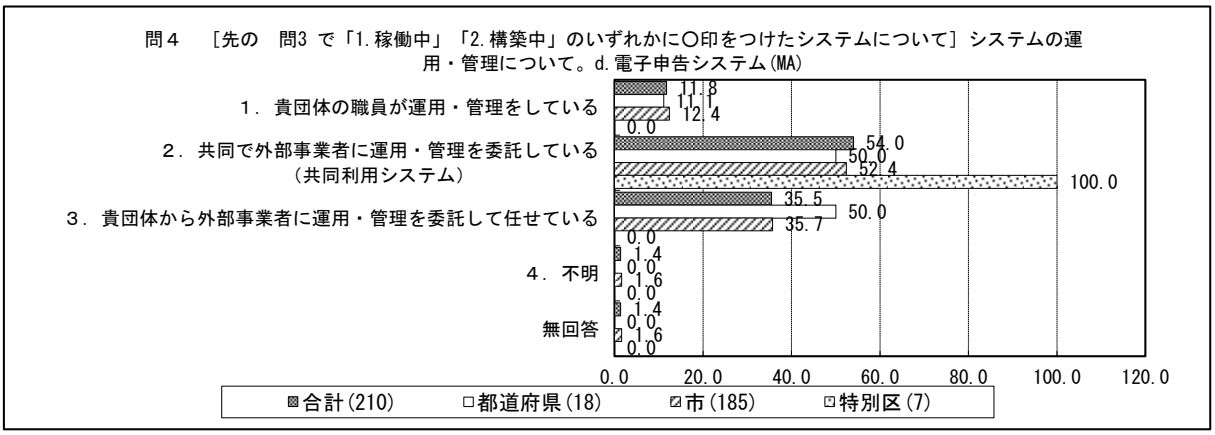

図 3.2-16　システムの運用・管理の主体について(d.電子申告システム)

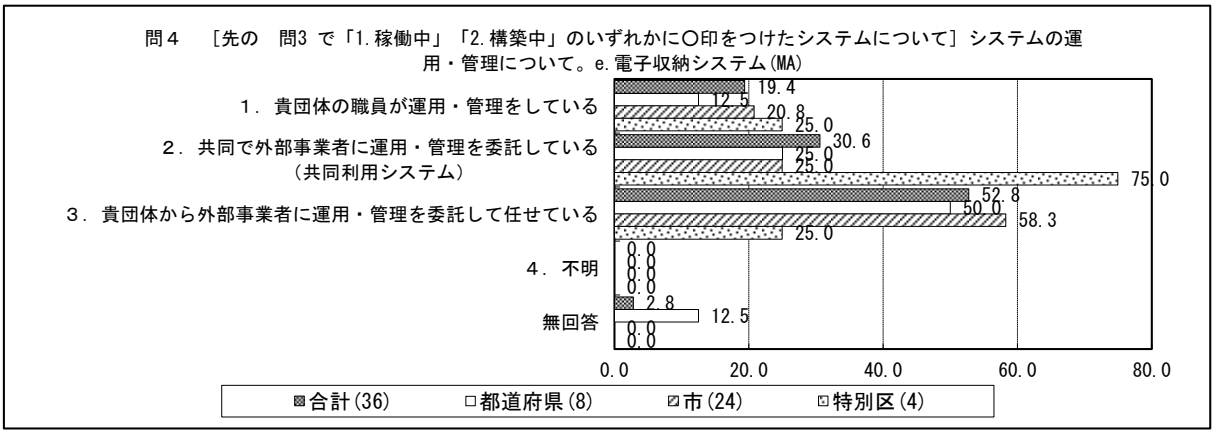

図 3.2-17　システムの運用・管理の主体について(e.電子収納システム)

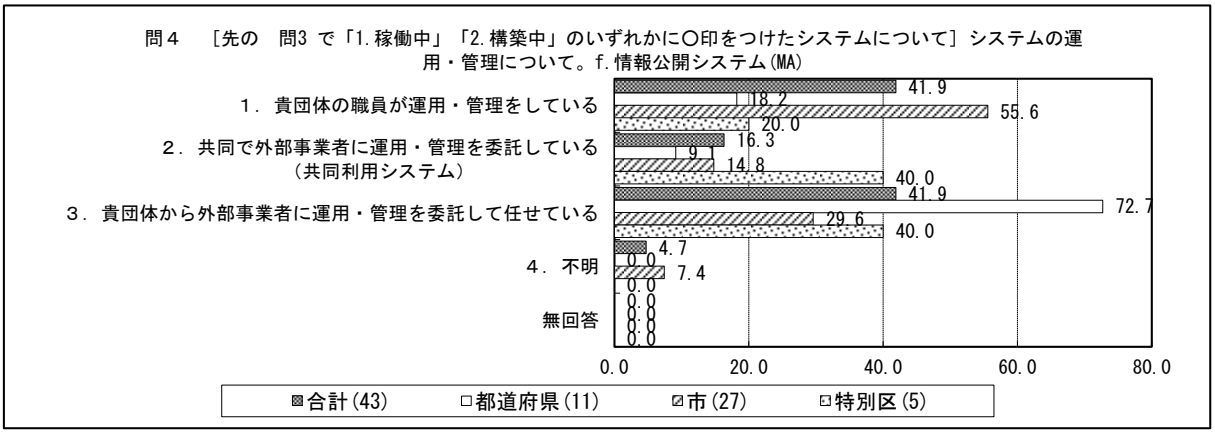

図 3.2-18　システムの運用・管理の主体について(f.情報公開システム)

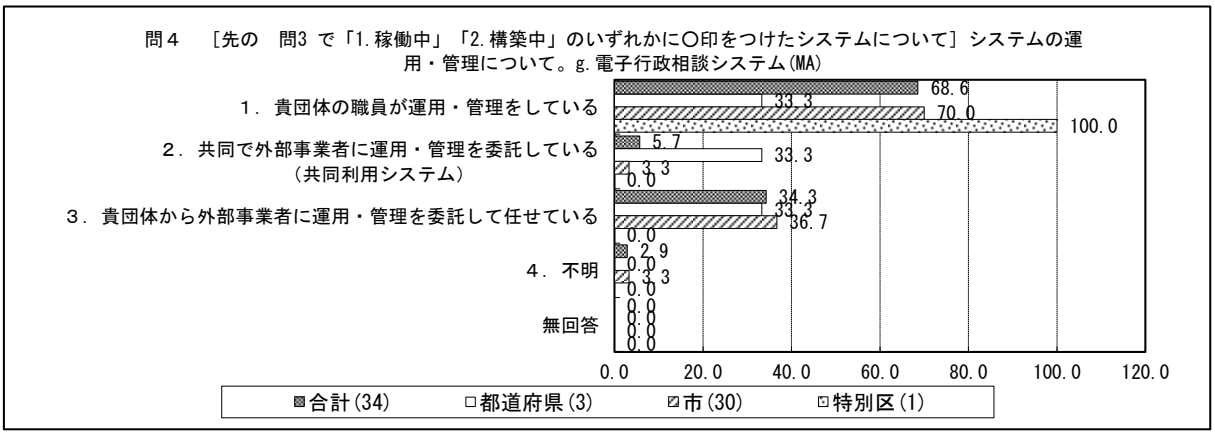

図 3.2-19　システムの運用・管理の主体について(g.電子行政相談システム)

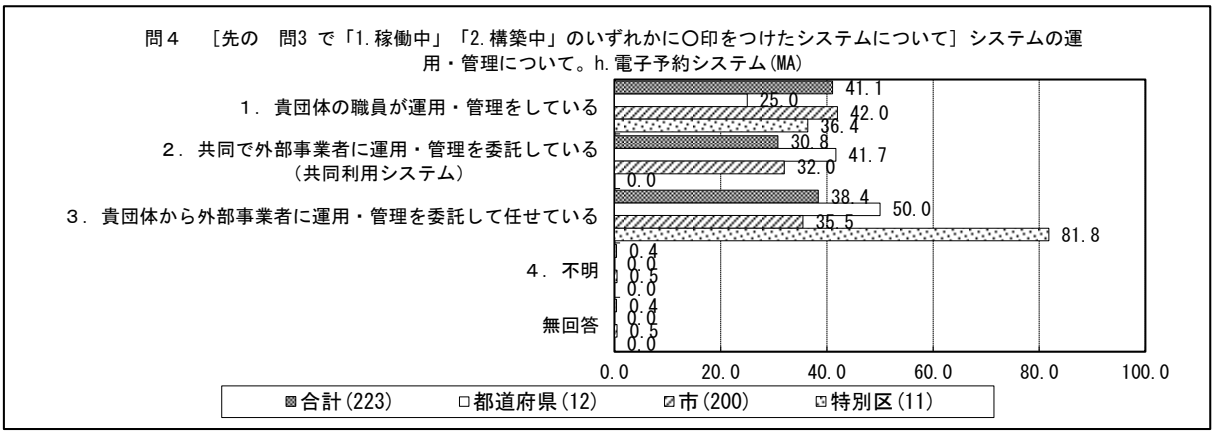

図 3.2-20　システムの運用・管理の主体について(h.電子予約システム)

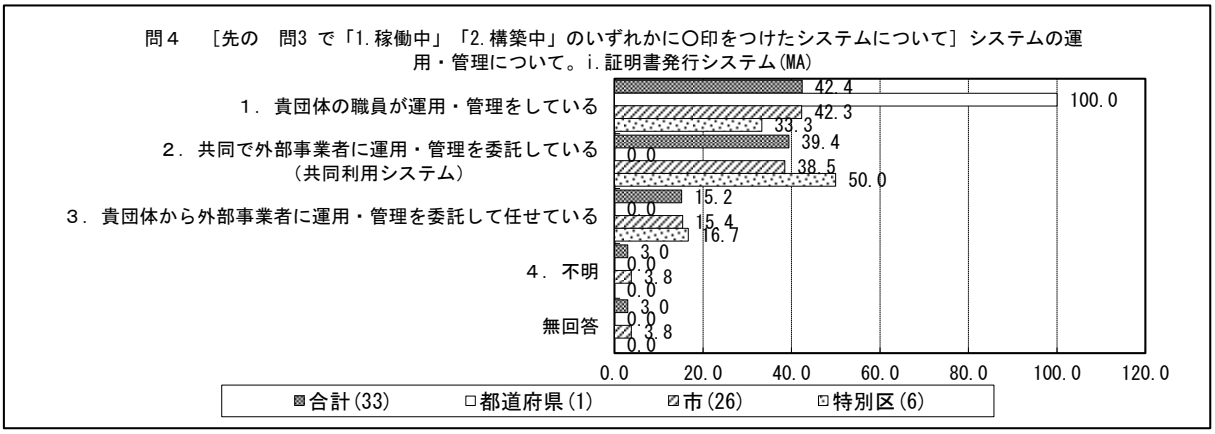

図 3.2-21　システムの運用・管理の主体について(i.証明書発行システム)

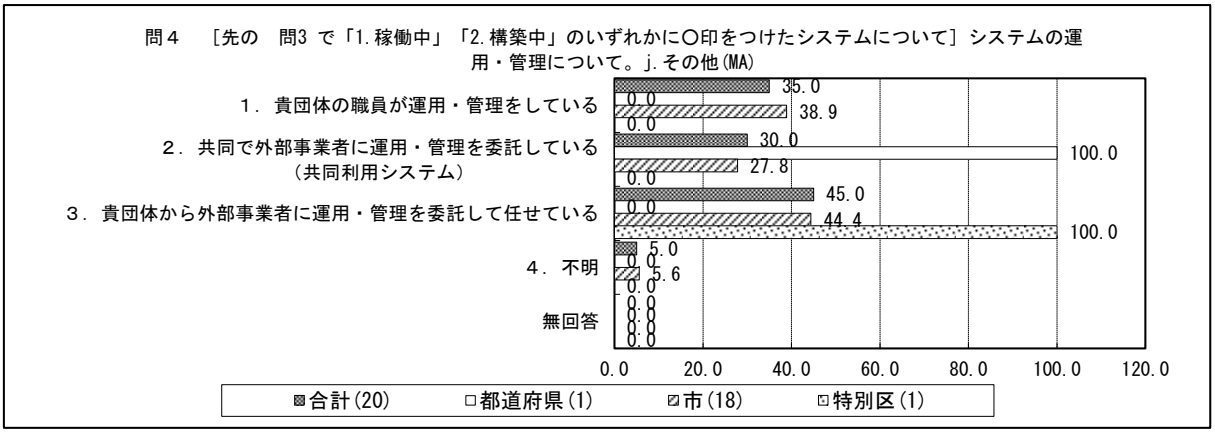

図 3.2-22　システムの運用・管理の主体について(j.その他)

3.2.5.ウェブサイトのセキュリティ管理の組織的な実施について

都道府県、市、特別区ともウェブサイトの管理を担当する部門（課）を有することが多い（それぞれ、66.7%、74.6%、72.7%）。都道府県は、各システムの担当者が対応している場合も 12.5%ある。

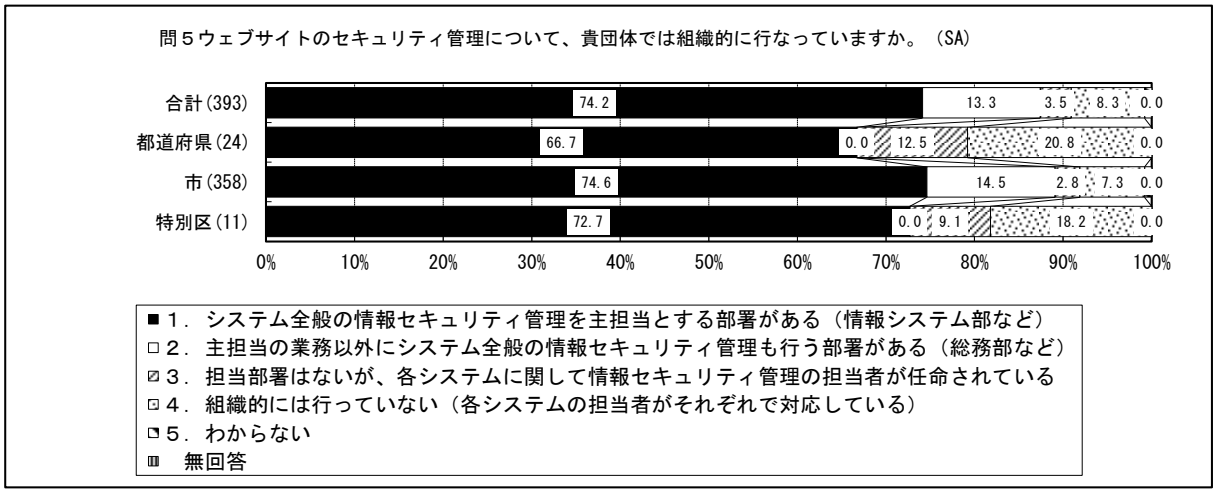

図 3.2-23　ウェブサイトのセキュリティ管理の組織的な実施

3.2.6.脆弱性に関する情報の収集・確認をする人員について

脆弱性に関する情報の収集・確認は専任担当者または情報システム部門の職員が担当しているケースが、都道府県で 62.5%、市で 75.2%、特別区で 72.7%と高い割合を占める。都道府県では、原課(オーナー部門)に委ねられている割合が 12.5%と、他の区分に比べ高い。

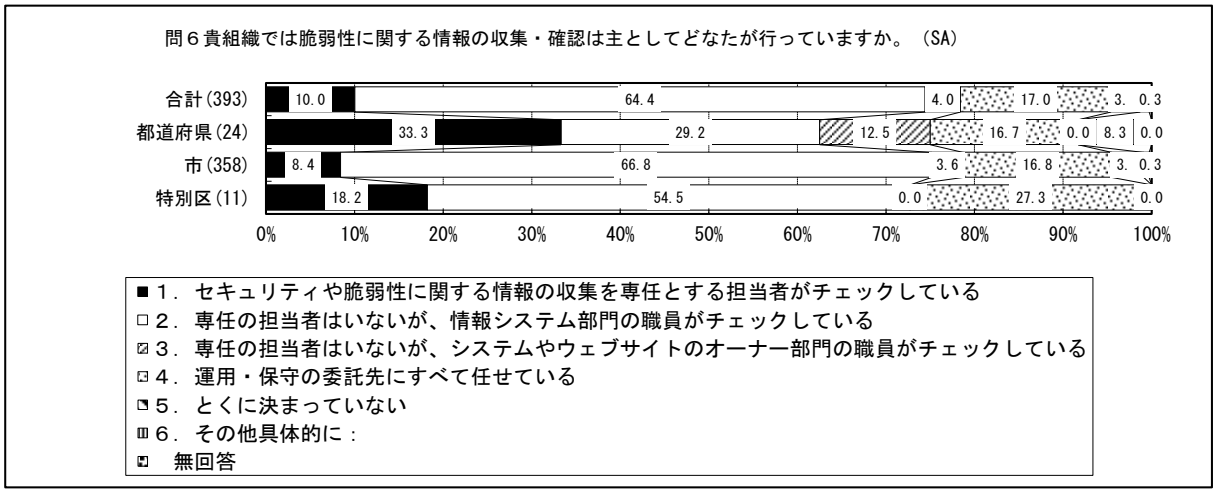

図 3.2-24　脆弱性に関する情報の収集・確認をする人員

3.2.7.脆弱性に関する情報の入手元について

自治体区分によらず、9 割以上の地方公共団体が『4.自治体セプター(LASDEC)』の情報を活用している（図 3.2-25)。

また、『5.その他の国内のセキュリティ関連組織・ボランティア等（IPA、JPCERT/CC の注意喚起、「セキュリティ memo」等のウェブサイトの情報など)』を活用すると回答する地方公共団体は、人口が多いほど高い割合になる傾向にある(図 3.2-26)。

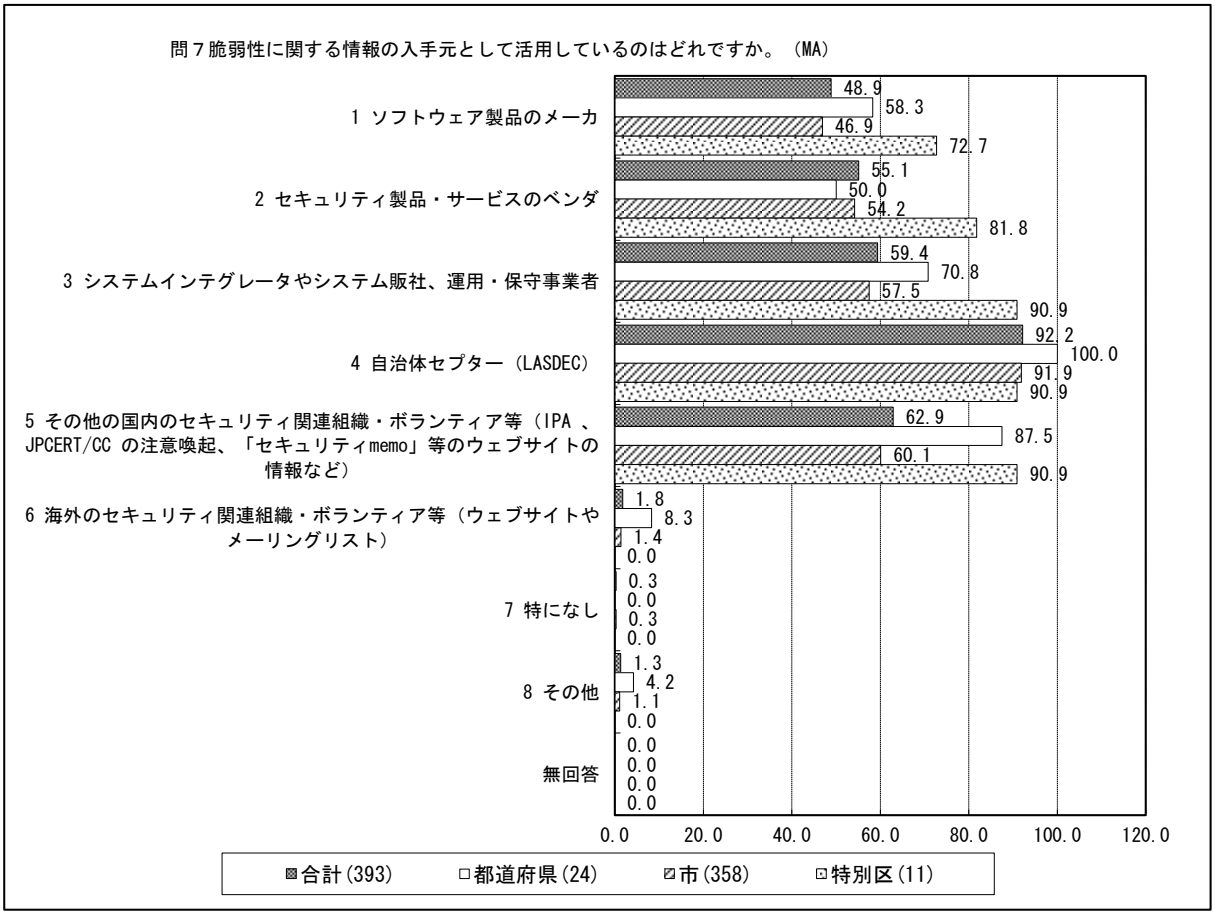

図 3.2-25　脆弱性に関する情報の入手元について

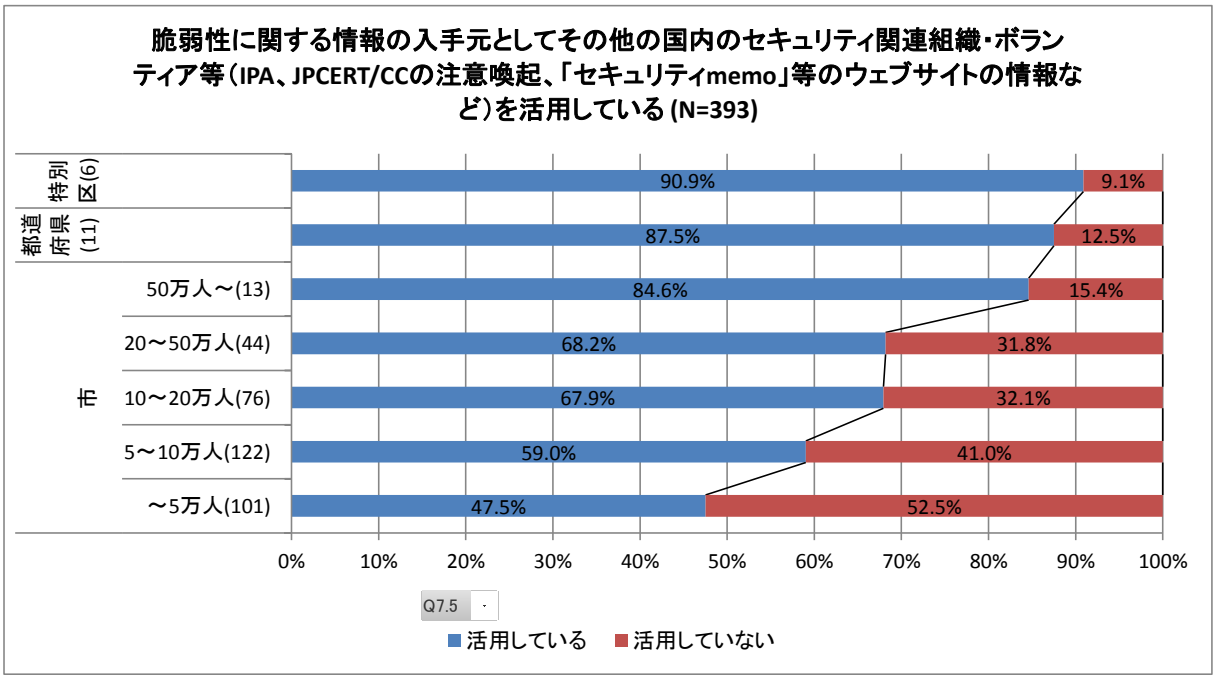

図 3.2-26　脆弱性に関する情報の入手元としてその他の国内のセキュリティ関連組織・ボランティア等（IPA、JPCERT/CC の注意喚起、「セキュリティ memo」等のウェブサイトの情報など）を活用しているかどうか

3.2.8.ウェブサイトを構築する際に実施する脆弱性対策について

特別区では、『1.仕様に脆弱性対策に関する項目を含めている』という対策を 100%実施している。『2.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』も 81.8%実施されており、対策が進んでいる。

ただし、『4.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』を選択した地方公共団体は、全体の 11.3%に過ぎず、脆弱性検査や診断を実施している組織はまだ少ない。

一方、『7.特に決まっていない』を選択した地方公共団体も、市で 28.8%、都道府県で 20.8%と、決して少なくない割合を占めている。

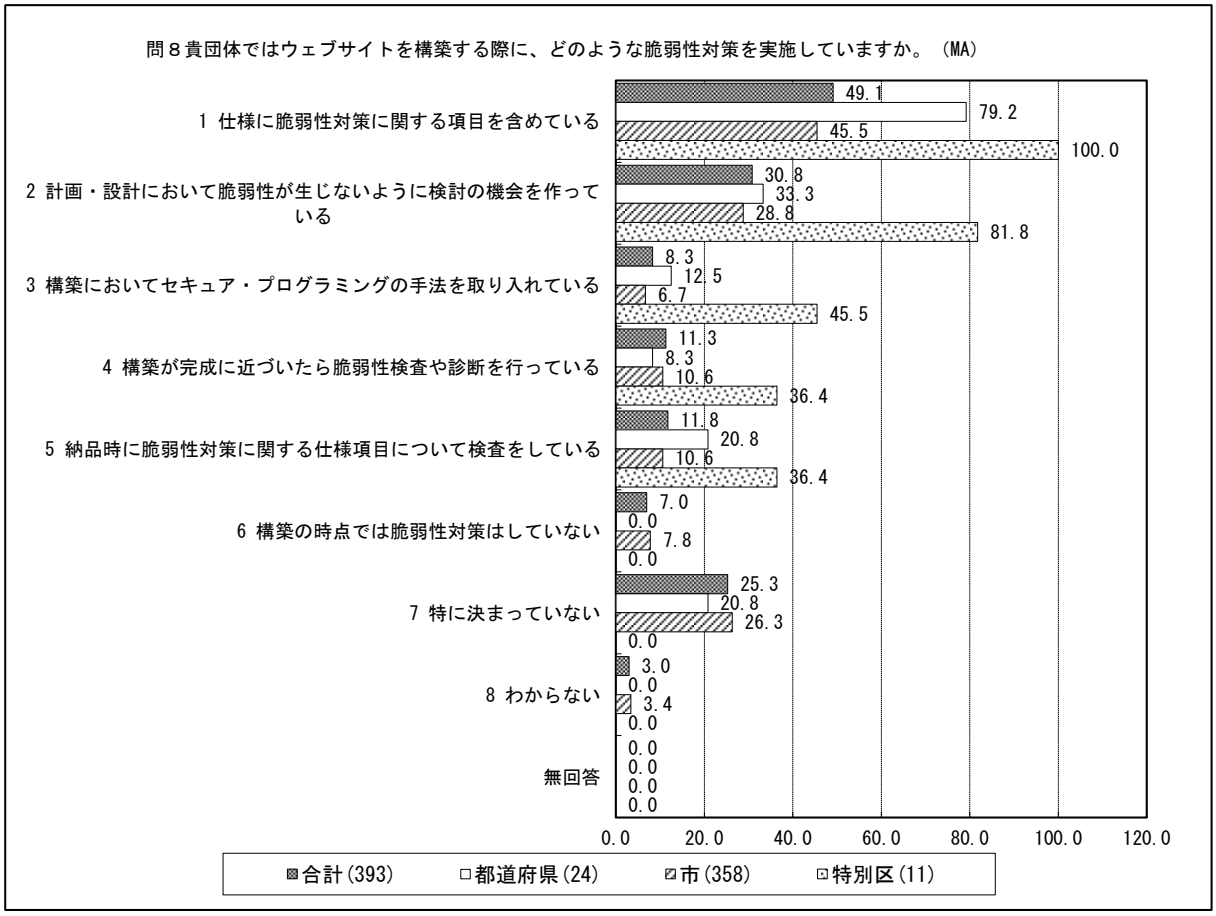

図 3.2-27　ウェブサイトを構築する際に実施する脆弱性対策

3.2.9.運用中のウェブサイトの脆弱性検査や脆弱性診断サービス利用状況について

『2.LASDEC（財団法人地方自治情報センター）の提供する脆弱性診断サービスを利用している』と回答した地方公共団体は、都道府県が 70.8%、氏が 75.7%、特別区が 54.5%といずれも高い割合を占める。

また、『3.その他の外部事業者の提供する脆弱性診断サービスを利用している』という回答は、特別区が 45.5%、都道府県が 37.5%と、市の 17.0%に比べて高い。

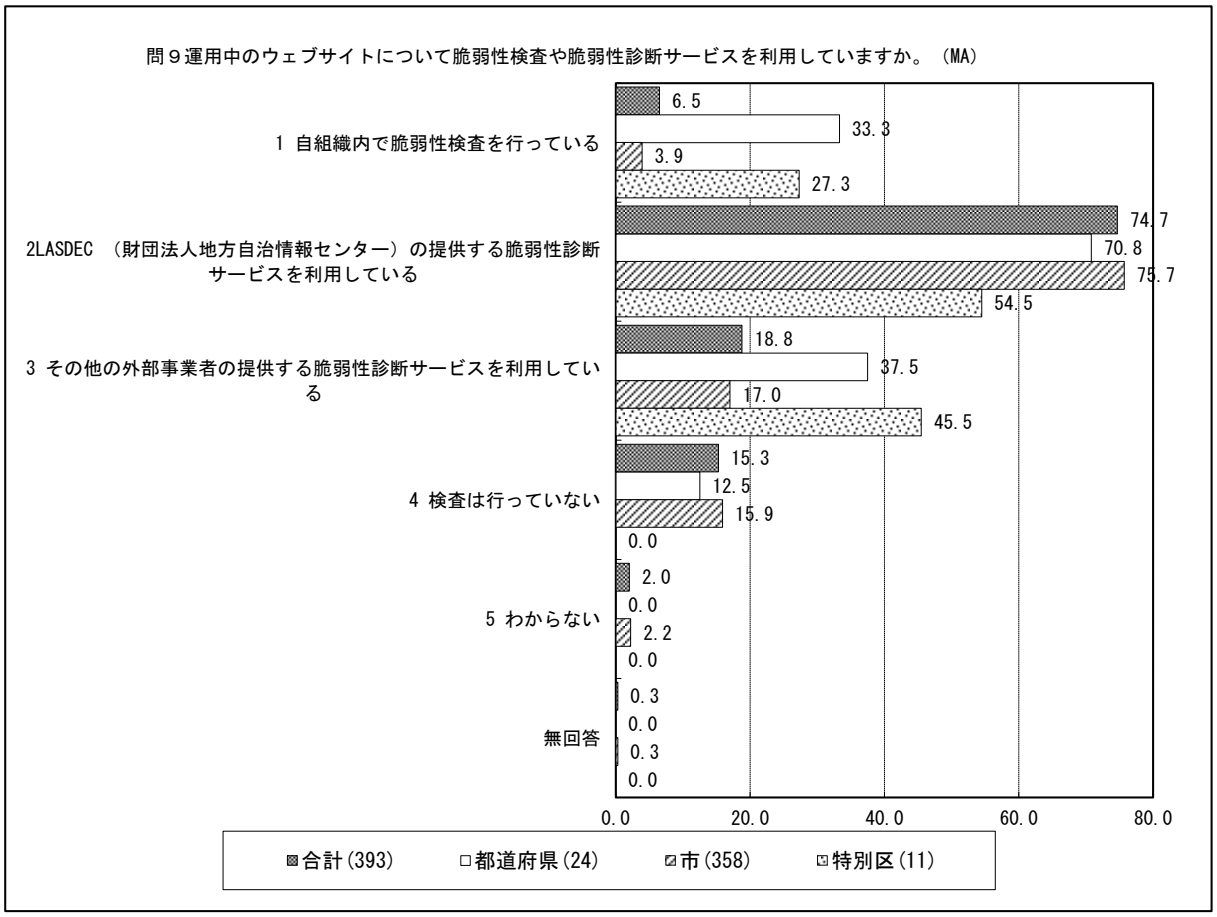

図 3.2-28　運用中のウェブサイトの脆弱性検査や脆弱性診断サービス利用状況

3.2.10.脆弱性検査や診断サービス利用の頻度について

[3.2.9で 1.～3.を回答した場合]

脆弱性の検査を定期的に実施していると回答した地方公共団体は、都道府県で 81.0%、市で 67.4%、特別区で 72.7%と非常に高い割合に占める。これは、LASDEC（財団法人地方自治情報センター）の提供する脆弱性診断サービスであると推測される。検査は、年に 1～2 回程度(平均 1.53 回)行われることが多い。

また、不定期に実施している地方公共団体も 25.1%存在する。

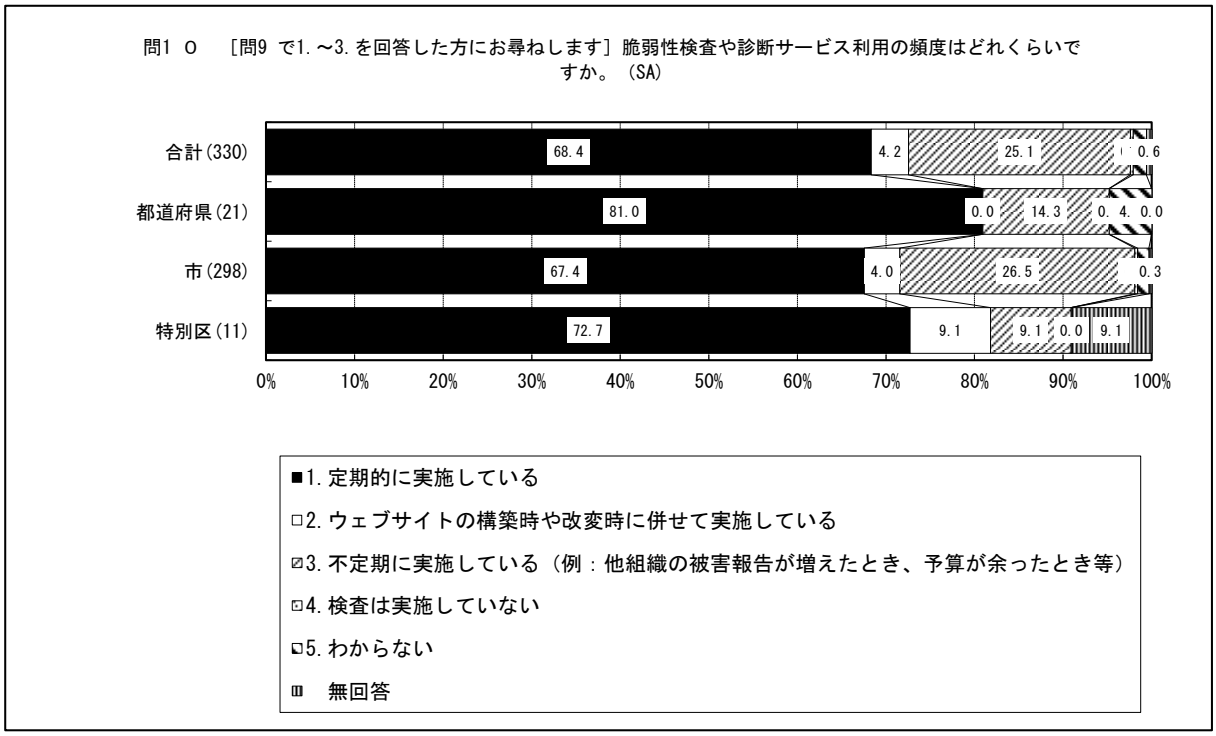

図 3.2-29 脆弱性検査や診断サービス利用の頻度

表 3.2-1 定期的に実施している場合の毎年の実施回数

		定期的に実施している方は具体的に年何回実施していますか	
		サンプル数	平 均
自治体区分	サンプル数	205	1.53
		100.0	
	都道府県	13	1.06
		6.3	
	市	184	1.59
		89.8	
	特別区(東京23区)	6	1.05
		2.9	
	無回答	2	1.00
		1.0	

3.2.11.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く、きっかけについて

『5.脆弱性検査や脆弱性診断サービスを通じて発見した』と回答する割合が最も高く、都道府県で 87.5%、市で 50.3%、特別区で 72.7%に達している。都道府県と特別区は、『6.脆弱性による情報を入手して、自組織で確認し発見した』、『4.セキュリティ関連組織（IPA、JPCERT/CC 等）から連絡を受けた』という場合も、都道府県で 54.2%、市で 32.1%、特別区で 45.5%が該当している。

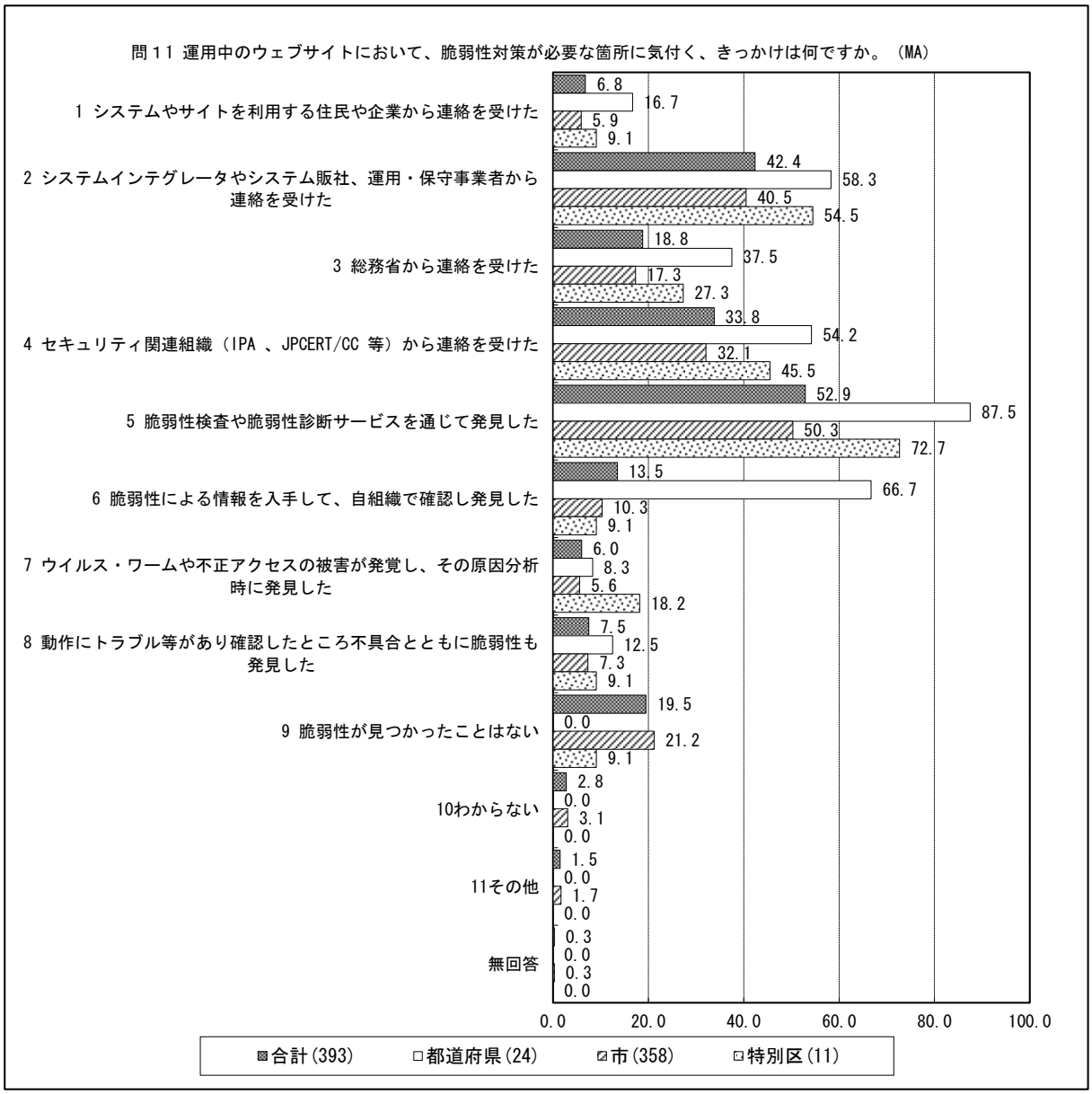

図 3.2-30　運用中のウェブサイトにおいて、脆弱性対策が必要な箇所に気付く、きっかけ

3.2.12.ウェブサイトの脆弱性について、脆弱性対策を適用すべきか否か等を判断する場合の参考情報について

『3.システムインテグレータ、システム販社、運用・保守事業者の意見』と回答した地方公共団体は、区分によらず高い割合を示しており、特に特別区は 81.8%である。『4.セキュリティ関連組織等が提供する情報（IPA 、JPCERT/CC 、CERT/CC の注意喚起等)』も高く、特に都道府県では 75.0%と最も高い割合にある。

さらに、特別区では、『2.ソフトウェア製品のメーカが提供する脅威および修正適用に伴う影響の情報』が 63.6%%と高い。

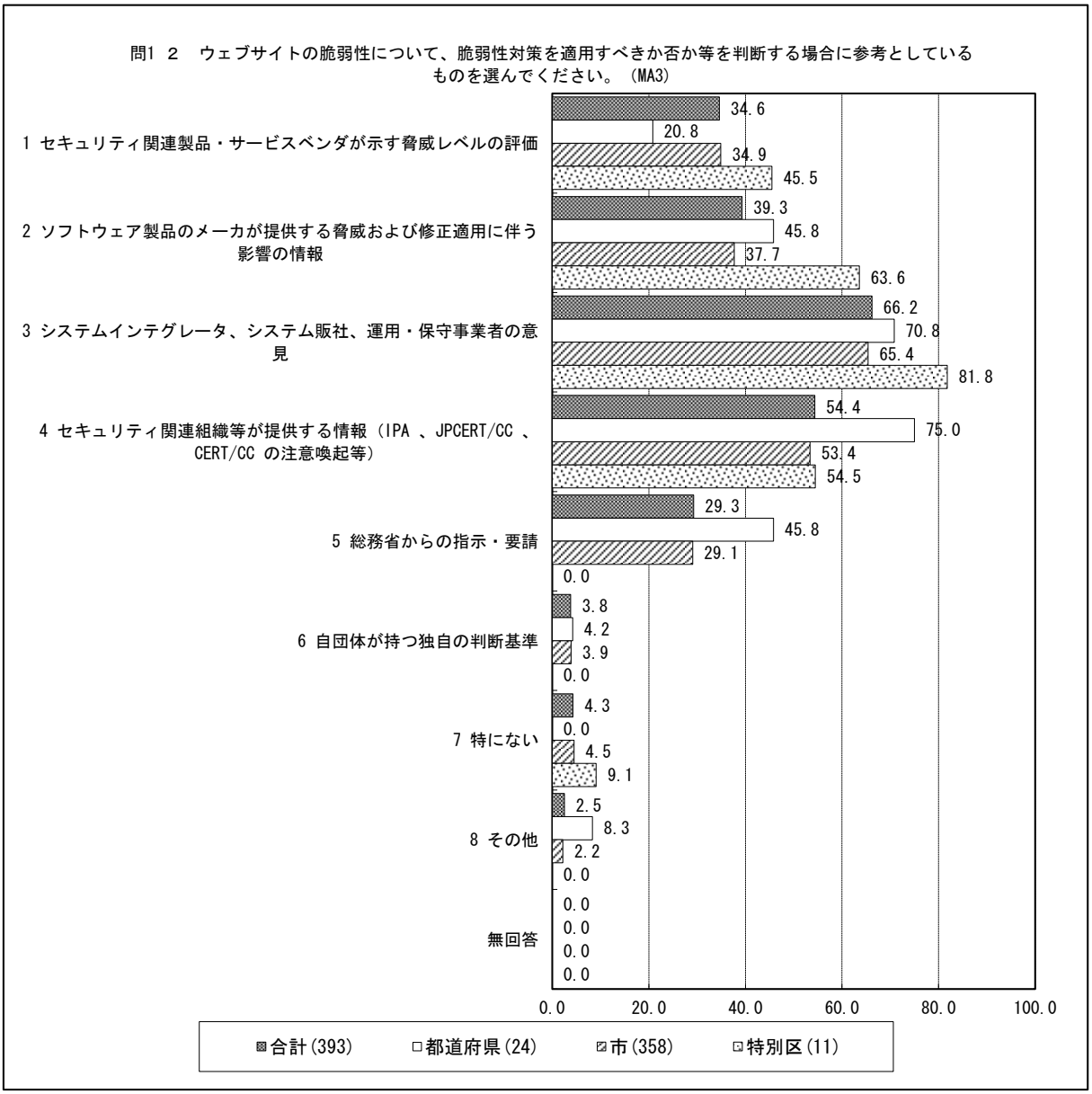

図 3.2-31 脆弱性の対策をするかどうかの判断に際して参考にする情報源[5]

[5]図中の設問部に記された「(MA3)」は、アンケートの質問が、複数回答方式であり、最大 3 項目にまで回答できることを示す。

3.2.13.ウェブサイトの脆弱性について、脆弱性対策を適用すべきか否か等を判断[6]する人について

『2.情報セキュリティ管理の担当部署の責任者』、『3.情報セキュリティ管理の実施担当者』がそれぞれ 62.4%、51.4%と高い。特に、特別区は『2.情報セキュリティ管理の担当部署の責任者』が 81.8%と高い。

都道府県では、『5.システムのオーナー部門の責任者』『6.システムのオーナー部門の運用担当者』が判断することも 50.0%、45.8%と高い。また、『7.委託先（システムインテグレータ、運用・保守事業者等)』を選択する場合も 45.8%と高い。『7.委託先』では、ホスティングサービスで委託先の運用事業者が脆弱性対策を行う仕組みになっているものも含むと考えられる。

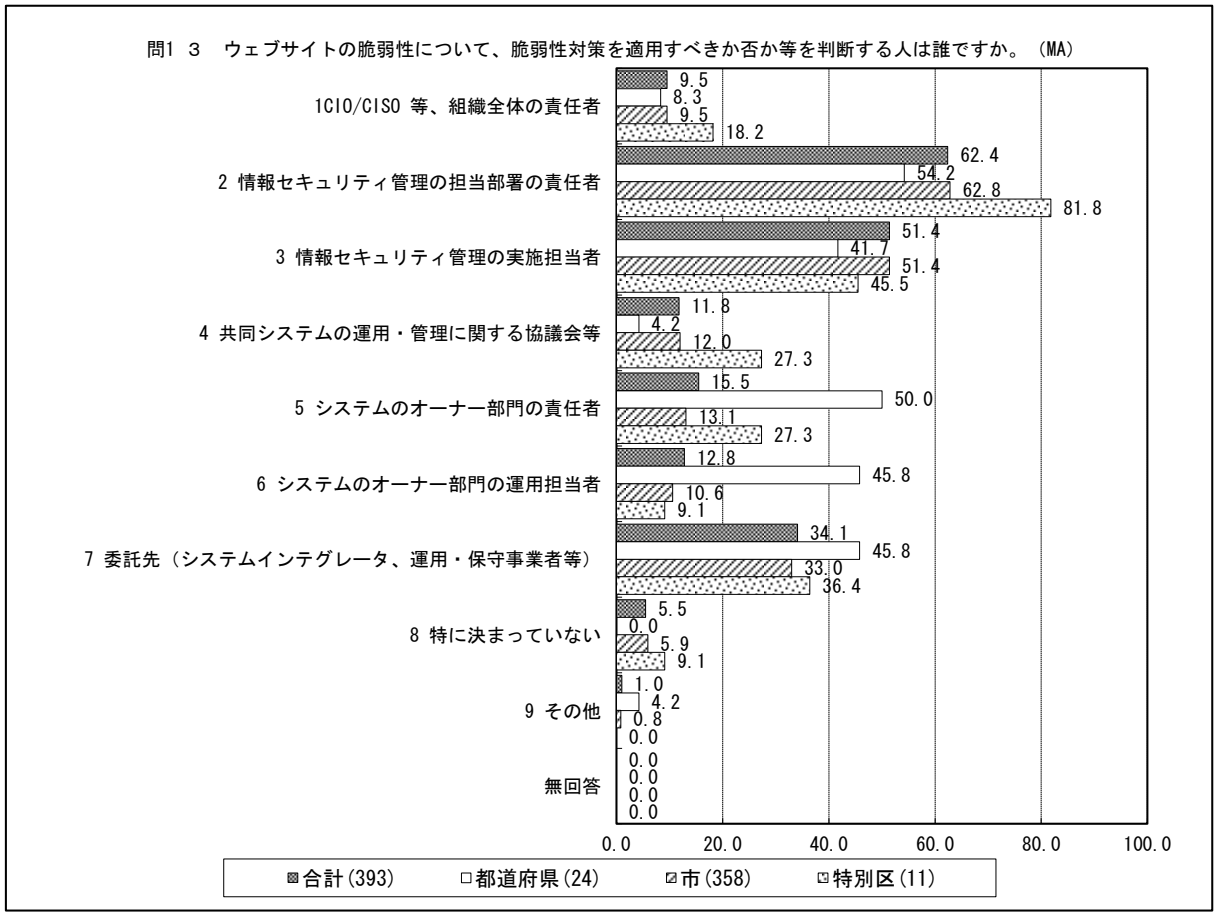

図 3.2-32 ウェブサイトの脆弱性について、脆弱性対策を適用すべきか否か等を判断する人

[6] 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とする。

3.2.14.運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応について

『1.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知するが、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ。』は、5.0%が選択した（図3.2-33）。この場合、対策が適用される前に公表すると、システムが攻撃され住民の情報が流出するなどの被害が生じるリスクや他組織の類似システムが攻撃対象となるリスクがあるが、回答者がそれらのリスクを認識していない可能性がある。

『2.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知し、当該システムを安全のため対策完了までは停止する』については、35.1%が選択した（図3.2-33）。この場合、他組織の類似システムが攻撃対象となるリスクがあるが、回答者がそれらのリスクを認識していない可能性がある。

次に高いのは、『3.攻撃を受けるリスクを抑えるために脆弱性の存在については対策を適用するまで住民への公表を控え、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ』（31.1%）であった。

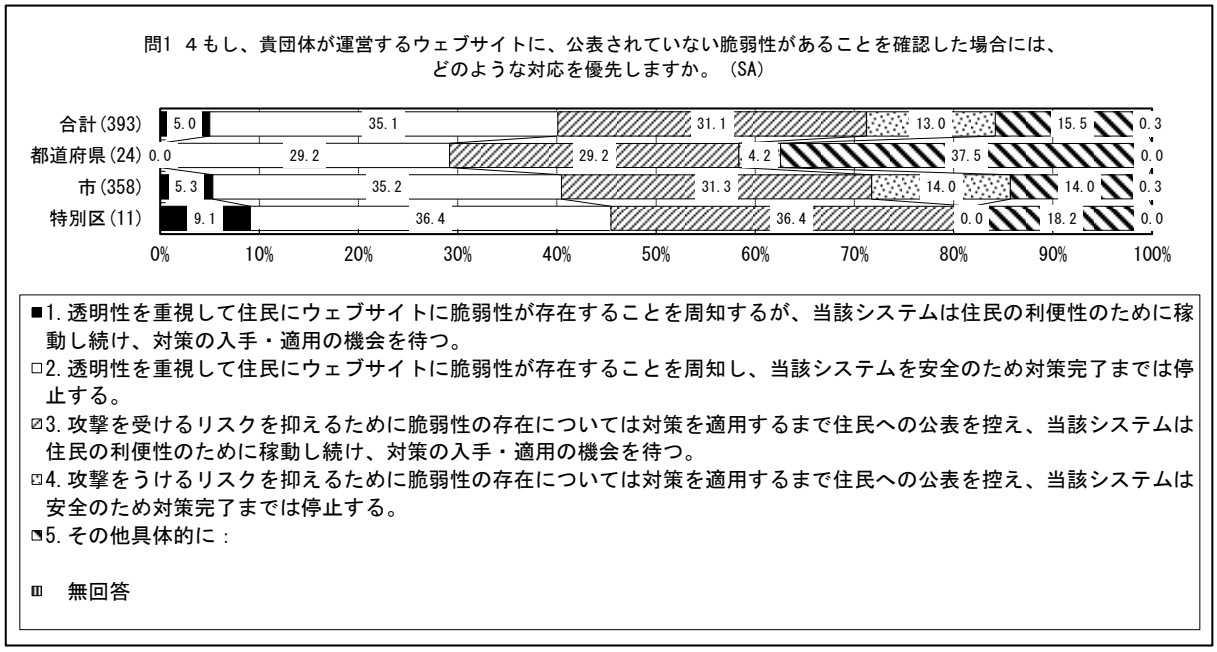

図 3.2-33　運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応

3.2.15. ［3.2.14で 1.を回答した場合］そのように判断する理由

情報公開原則に従うという、『1.住民や企業に対する透明性の確保が原則としてルールづけられているから』と回答した地方公共団体はすべて市で、25%であった。

『3.脆弱性の対策手段はシステムインテグレータや製品開発者から迅速に提供されるはずであるから』と回答した地方公共団体は 50%であった。本回答では、脆弱性の種類によっては改修に時間が掛かる場合もあるので注意が必要である。

表 3.2-2　［3.2.14で 1.を回答した場合］そのように判断する理由

		問1５［問14で1.を回答した方にお尋ねします］そのように判断する理由のうちあてはまるものを以下からお答えください。(MA)							
		合計	1 住民や企業に対する透明性の確保が原則としてルールづけられているから	2 脆弱性をサービスを停止する理由として考慮していないから	3 脆弱性の対策手段はシステムインテグレータや製品開発者から迅速に提供されるはずであるから	4 自組織のシステムやサイトが攻撃を受けるとは考えにくいから	5 脆弱性対策の予算請求について議会で了承をえる必要があるから	6 その他	無回答
自治体区分	合計	20 100.0	5 25.0	2 10.0	10 50.0	2 10.0	－ －	1 5.0	2 10.0
	都道府県	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －
	市	19 100.0	5 26.3	2 10.5	9 47.4	2 10.5	－ －	1 5.3	2 10.5
	特別区	1 100.0	－ －	－ －	1 100.0	－ －	－ －	－ －	－ －
	無回答	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －

3.2.16.ウェブサイトに関する脆弱性情報の収集、脆弱な箇所の特定と報告（外部からの発見報告を受領した場合を含む）、対処方針の決定、対策実施といった一連の手順の文書化状況について

都道府県と市では、『4.特に定まった手順はない』が、それぞれ 50.0%、62.3%と高い。

ただし、都道府県では、『1.組織内ルールとして文書化されており、その手順を活用している』場合も 37.5%と高く、特に定まった手順の無い都道府県と二分されている。

市では『1.組織内ルールとして文書化されており、その手順を活用している』割合は、16.5%にとどまっており、文書化は今後進められていくべきと言える。

なお、被害経験(3.2.17)の有無との関係は、図 3.2-35に示す通り。被害経験があり『1.組織内ルールとして文書化されており、その手順を活用している』割合は 25.5%と高い(全体では 18.3%)。

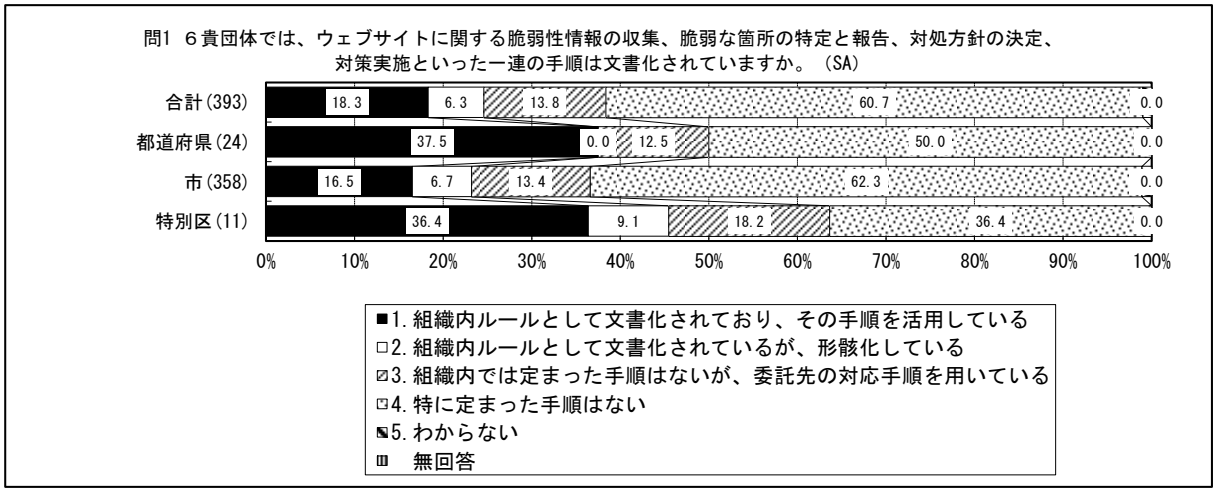

図 3.2-34 ウェブサイトに関する脆弱性情報の収集、脆弱な箇所の特定と報告（外部からの発見報告を受領した場合を含む）、対処方針の決定、対策実施といった一連の手順の文書化状況

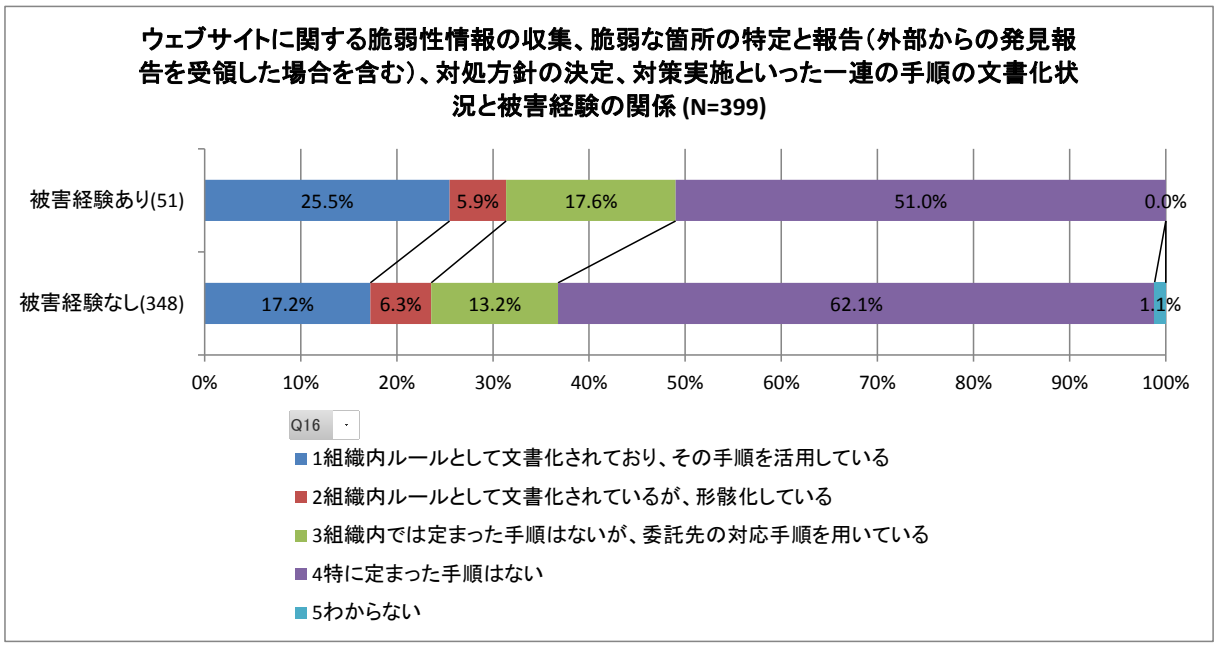

図 3.2-35　ウェブサイトに関する脆弱性情報の収集、脆弱な箇所の特定と報告（外部からの発見報告を受領した場合を含む）、対処方針の決定、対策実施といった一連の手順の文書化状況と被害経験の関係

3.2.17.ウェブサイトの脆弱性対策の適用の判断が遅れたり誤ったりしたため、ワームや不正アクセス等の被害に遭った経験の有無について

被害経験の無い地方公共団体が 85%程度だが、都道府県では一部の業務に影響が生じる程度の被害を受けた経験を持つところも 20.8%ある。また、人口の多い地方公共団体ほど、被害経験がある傾向にある(図 3.2-37)。

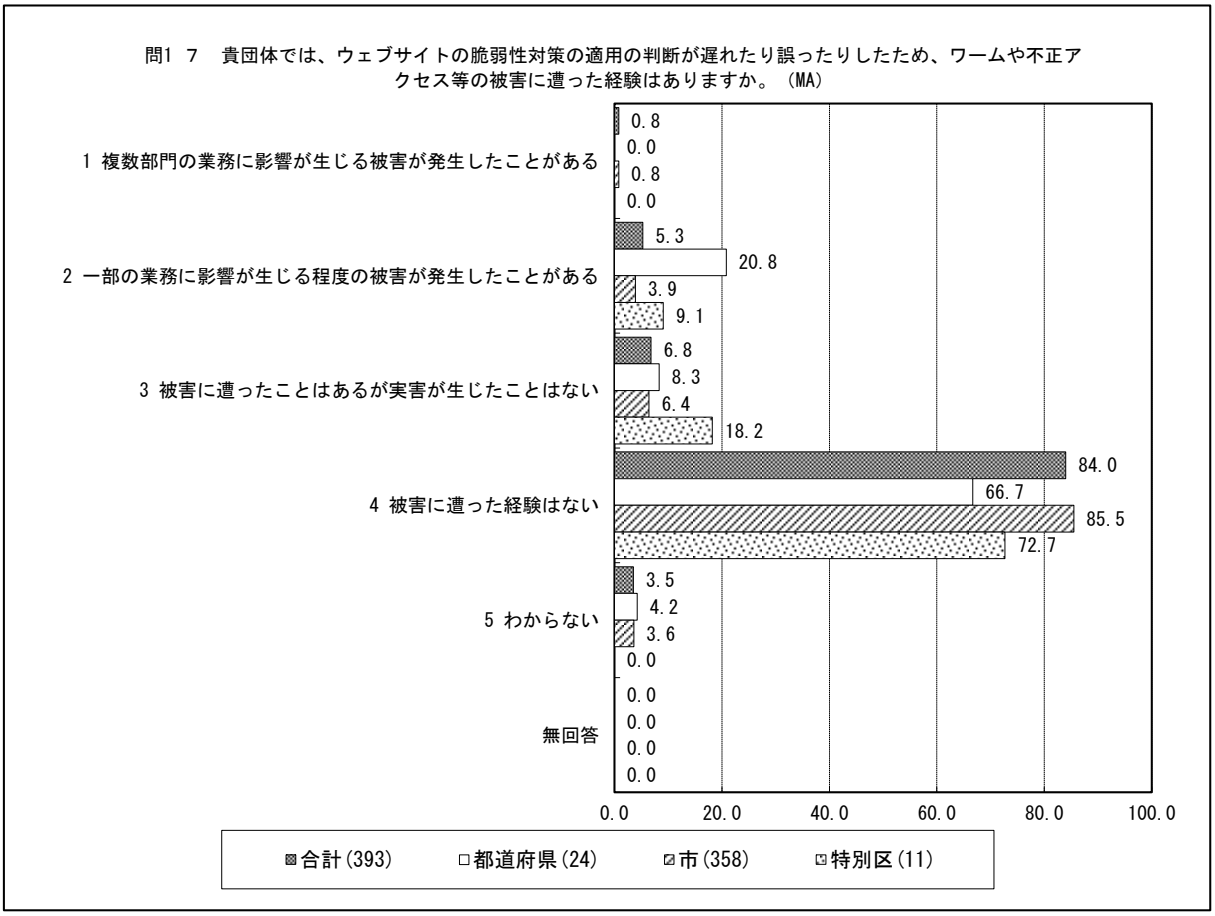

図 3.2-36 ウェブサイトの脆弱性対策の適用の判断が遅れたり誤ったりしたため、ワームや不正アクセス等の被害に遭った経験の有無

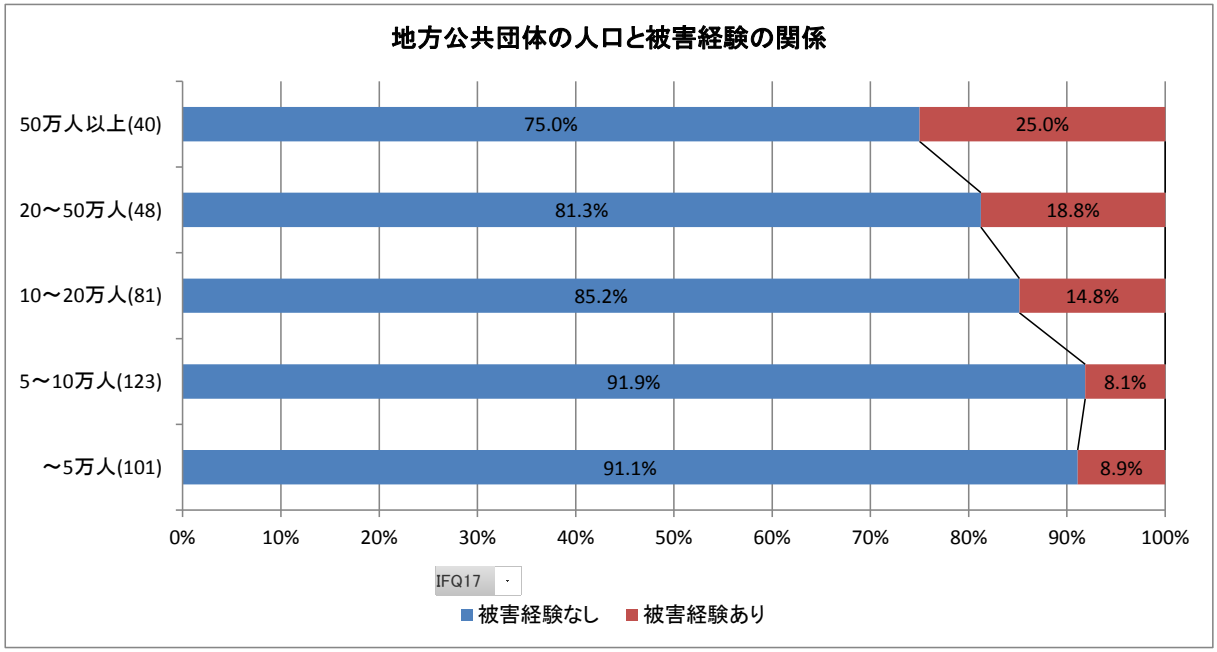

図 3.2-37　地方公共団体の人口と被害経験の関係

3.2.18.運用中のウェブサイト上で発覚した脆弱性について、問題箇所の修正や回避策の適用等（含テスト）の作業の担当について

運用中のウェブサイト上で発覚した脆弱性について、問題箇所の修正や回避策の適用等（含テスト）の作業については、『4.委託先の運用・保守事業者』が実施する割合が最も高く 74.4%である。特に、特別区はその傾向が強い。また、図 3.2 38 から、人口の多い市ほど委託先が担当する割合が高くなる。

市の一部(10.1%)では、『1.情報セキュリティ管理の実施担当者』が担当している。また、都道府県には、『2.ウェブサイトのオーナー部門』が担当するところも 8.3%ある。

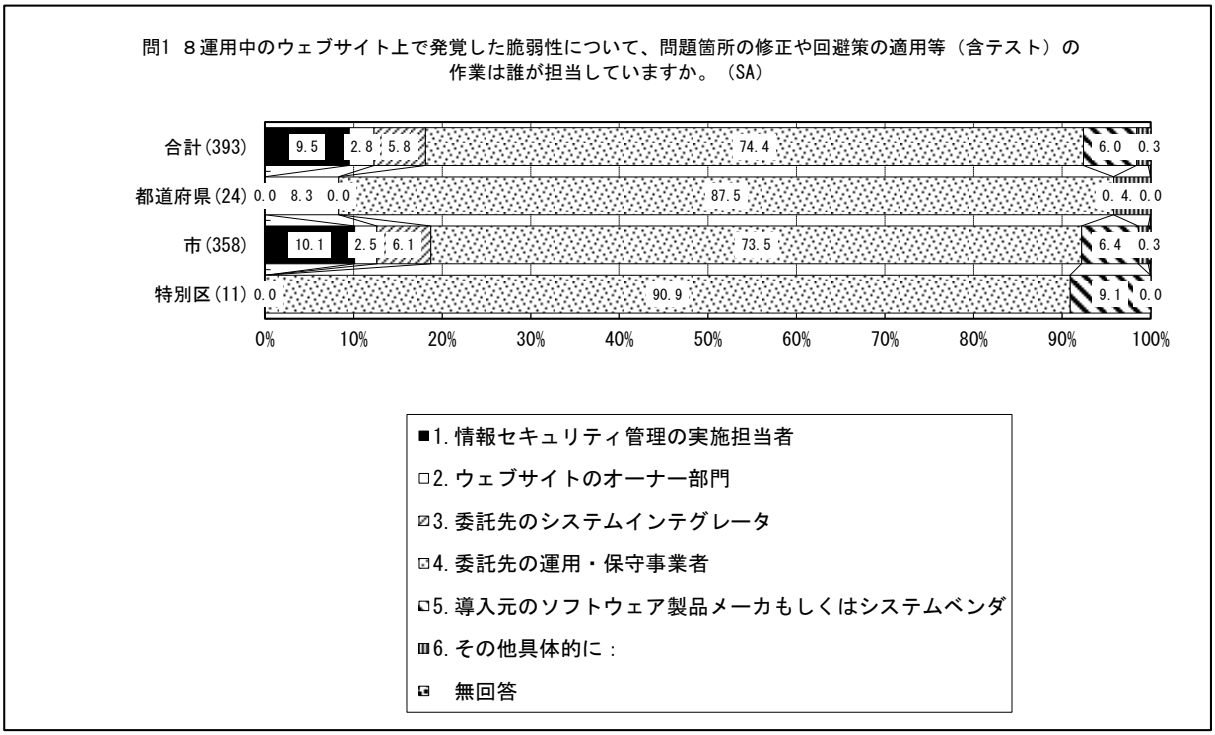

図 3.2-38 運用中のウェブサイト上で発覚した脆弱性について、問題箇所の修正や回避策の適用等（含テスト）の作業の担当について

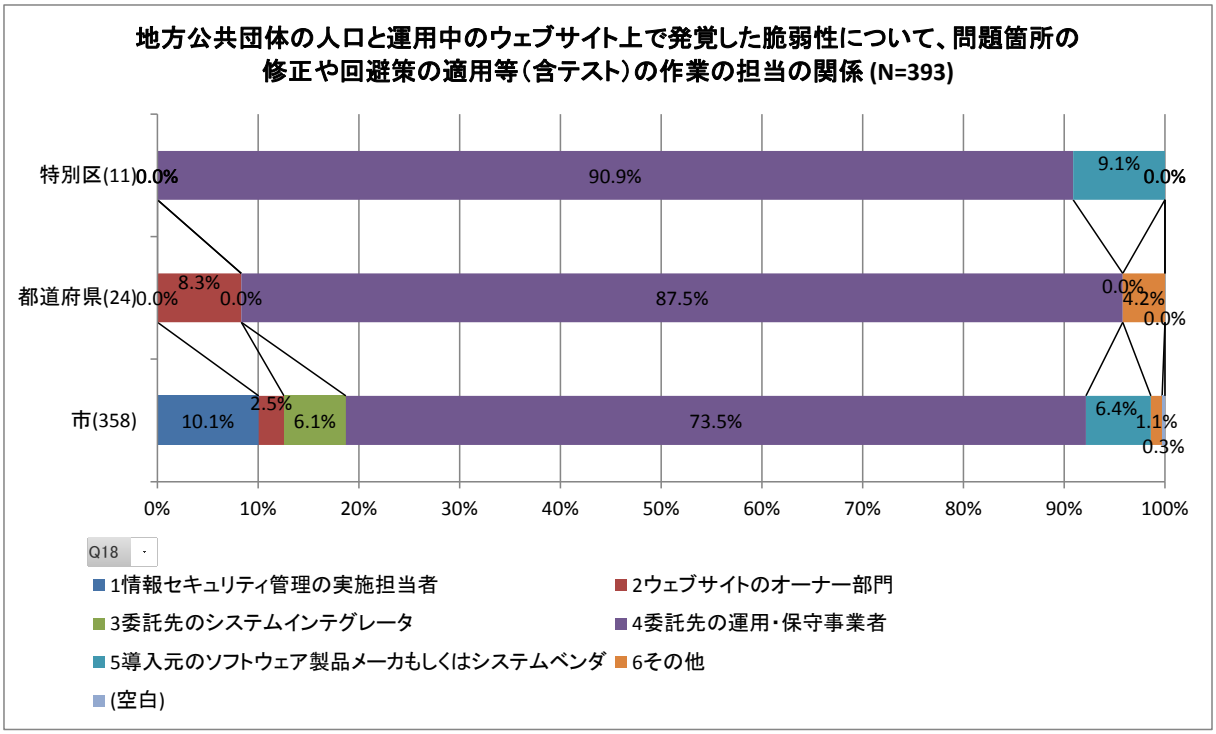

図 3.2-39　地方公共団体の人口と運用中のウェブサイト上で発覚した脆弱性について、問題箇所の修正や回避策の適用等（含テスト）の作業の担当の関係

3.2.19.運用中のウェブサイトの脆弱性対策に必要な費用の負担について
［3.2.18 で 3.～6.を回答した場合］

都道府県は、『1.脆弱性対策は委託先との契約に明記されており、委託費用に全て含まれている（個別の支払いはしていない)』の割合が 54.5%と多い。市では、『3.脆弱性対策は委託先との契約に明記されていないが、事実上、委託費用に全て含まれている（個別の支払いはしていない）』という割合が 38.1%になっている。ただし、ホスティングによるホームページの運用のみで、脆弱性管理もサービスに組み込まれている可能性がある。

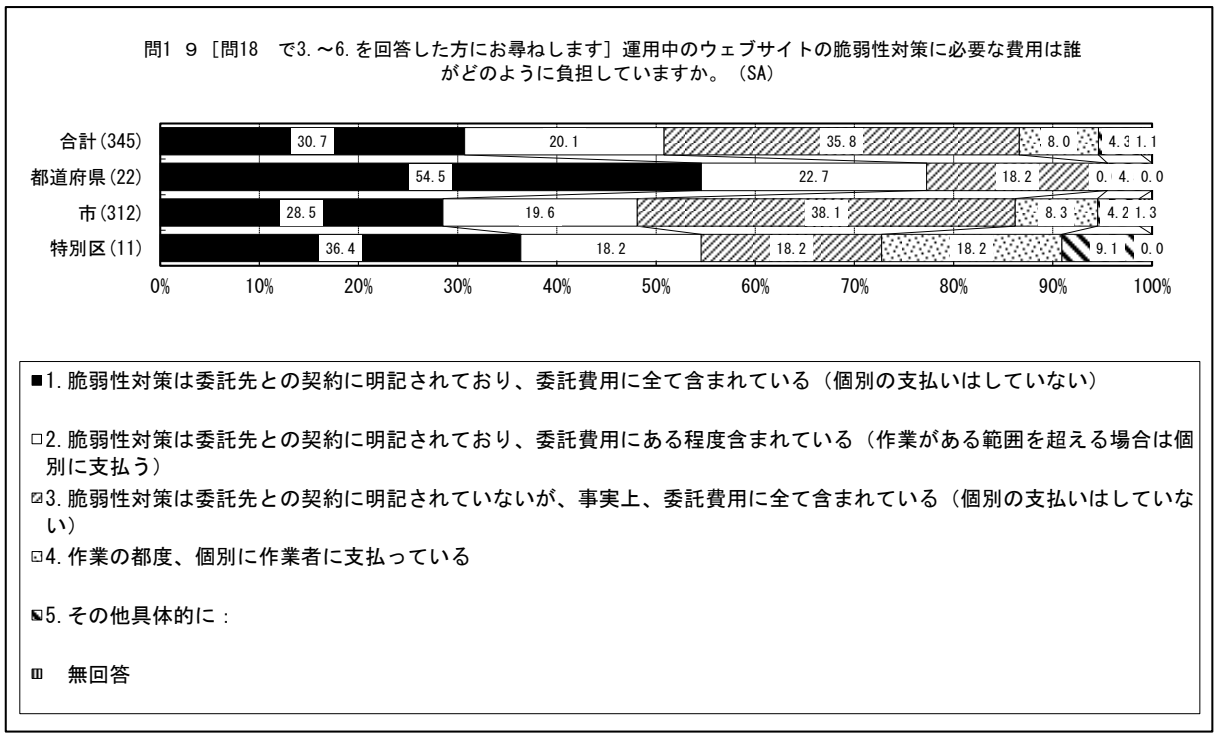

図 3.2-40 運用中のウェブサイトの脆弱性対策に必要な費用の負担について
［3.2.18 で 3.～6.を回答した場合］

3.2.20.ウェブサイトの脆弱性を修正するタイミングについて

『3.緊急性の高いものだけを即時実施し、それ以外は状況に応じて適宜実施』が 31.1%と多い。都道府県では、『2.緊急性の高いものは即時実施し、それ以外は複数の修正点とまとめて定期的に実施』が 45.8%と高い。

市では『5.状況に応じて適宜実施』が最も多く、34.1%であった。

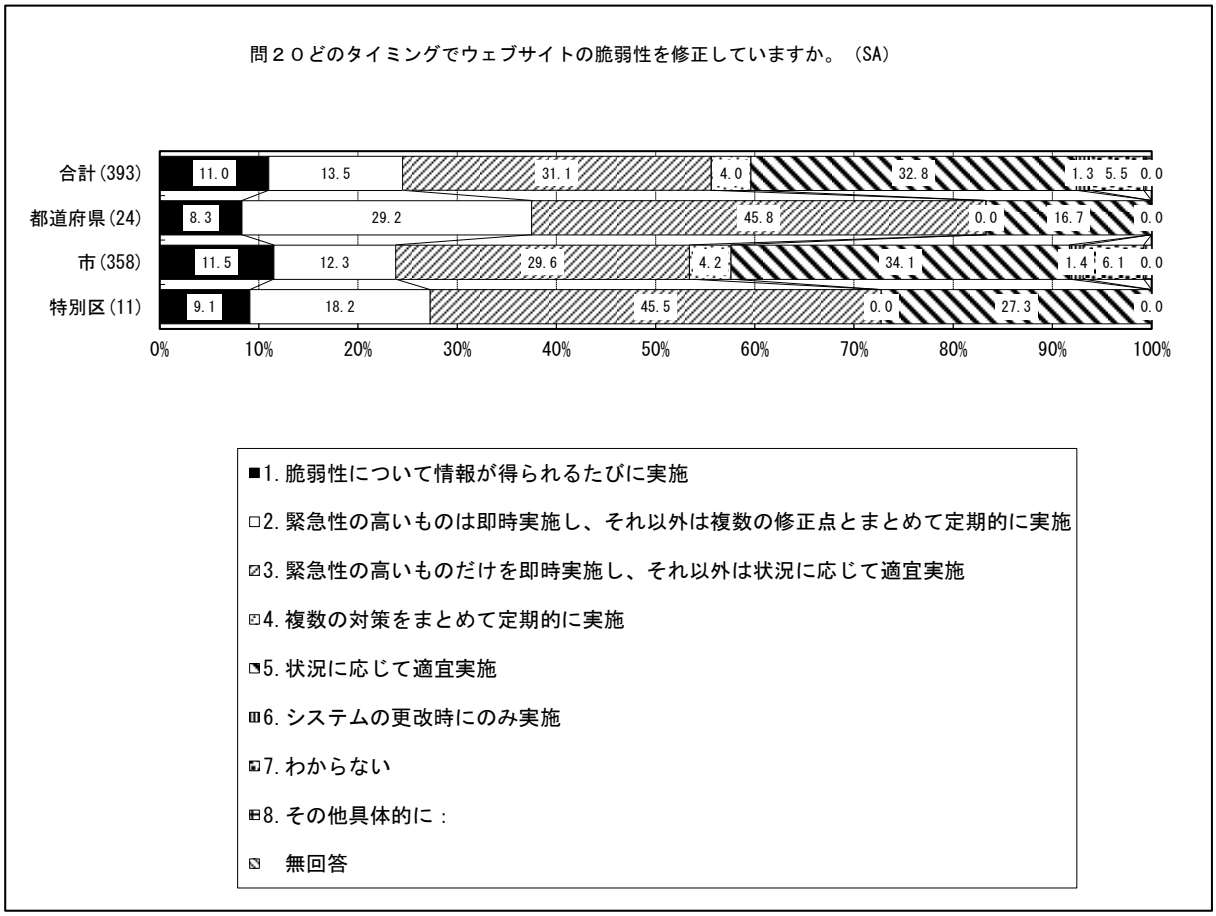

図 3.2-41　ウェブサイトの脆弱性を修正するタイミング

3.2.21. ウェブサイトのセキュリティ対策に必要な費用や人員の確保状況について

都道府県では 54.2%が、市では 42.2%が、特別区では 72.7%が、ウェブサイトのセキュリティ対策に必要な費用や人員を『2.おおむね確保できている』としている。それと同時に、都道府県と市の 40%程度は不足していると感じている。特に人口の少ない市を中心に『4.全く足りていない』という回答が 11.8%ある(4.3参照)。

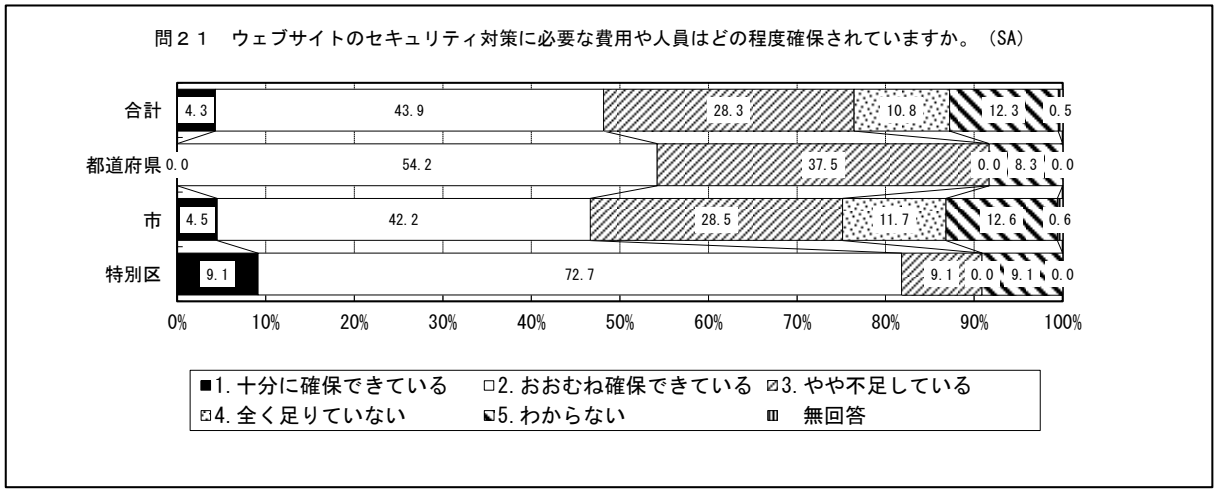

図 3.2-42　ウェブサイトのセキュリティ対策に必要な費用や人員の確保状況

3.2.22. ウェブサイト関連システムに脆弱性対策を進める上での課題について

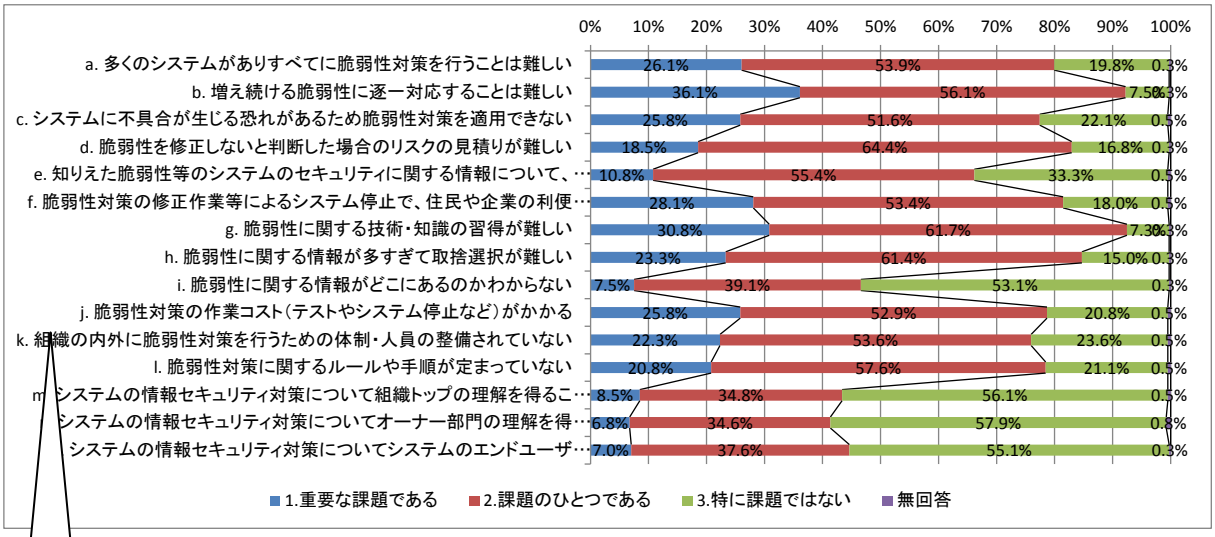

図 3.2-43　ウェブサイト関連システムに脆弱性対策を進める上での課題

	課題
a.	多くのシステムがありすべてに脆弱性対策を行うことは難しい
b.	増え続ける脆弱性に逐一対応することは難しい
c.	システムに不具合が生じる恐れがあるため脆弱性対策を適用できない
d.	脆弱性を修正しないと判断した場合のリスクの見積りが難しい
e.	知りえた脆弱性等のシステムのセキュリティに関する情報について、秘密にすべきか、住民や企業への透明性を重視して公開すべきかが悩ましい
f.	脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい
g.	脆弱性に関する技術・知識の習得が難しい
h.	脆弱性に関する情報が多すぎて取捨選択が難しい
i.	脆弱性に関する情報がどこにあるのかわからない
j.	脆弱性対策の作業コスト（テストやシステム停止など）がかかる
k.	組織の内外に脆弱性対策を行うための体制・人員の整備されていない
l.	脆弱性対策に関するルールや手順が定まっていない
m.	システムの情報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
n.	システムの情報セキュリティ対策についてオーナー部門の理解を得ることが難しい
o.	システムの情報セキュリティ対策についてシステムのエンドユーザ（住民や企業）の理解を得ることが難しい

・ 図 3.2-43より、次の項目が地方公共団体において『重要な課題である』として認識されていることがわかる。『f. 脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい』が上位に入ることはヒアリング結果[7]とも合致する。

b. 増え続ける脆弱性に逐一対応することは難しい	36.1%
g. 脆弱性に関する技術・知識の習得が難しい	30.8%
f. 脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい	28.1%

[7] 3.4.1小節参照

・ また、次の項目が地方公共団体において『課題のひとつである』として認識されている。『d. 脆弱性を修正しないと判断した場合のリスクの見積りが難しい』の割合が最も高く、「止めることの影響と、止めないことのリスクの判断になってくる」などのヒアリング結果とも合致する。

d. 脆弱性を修正しないと判断した場合のリスクの見積りが難しい	64.4%
g. 脆弱性に関する技術・知識の習得が難しい	61.7%
h. 脆弱性に関する情報が多すぎて取捨選択が難しい	61.4%

3.2.23.「情報セキュリティ早期警戒パートナーシップ」の取組みの認知度について

都道府県と特別区では、『2.聞いたことがあり、内容も良く知っている』割合が、20.8%、18.2%である。しかし、市では8.7%にとどまる。

一方、『4.聞いたことはない』という回答は、都道府県 20.8%、特別区 27.3%、市 34.4%となっている。市に対する広報活動が同パートナーシップの普及には必要と考えられる。

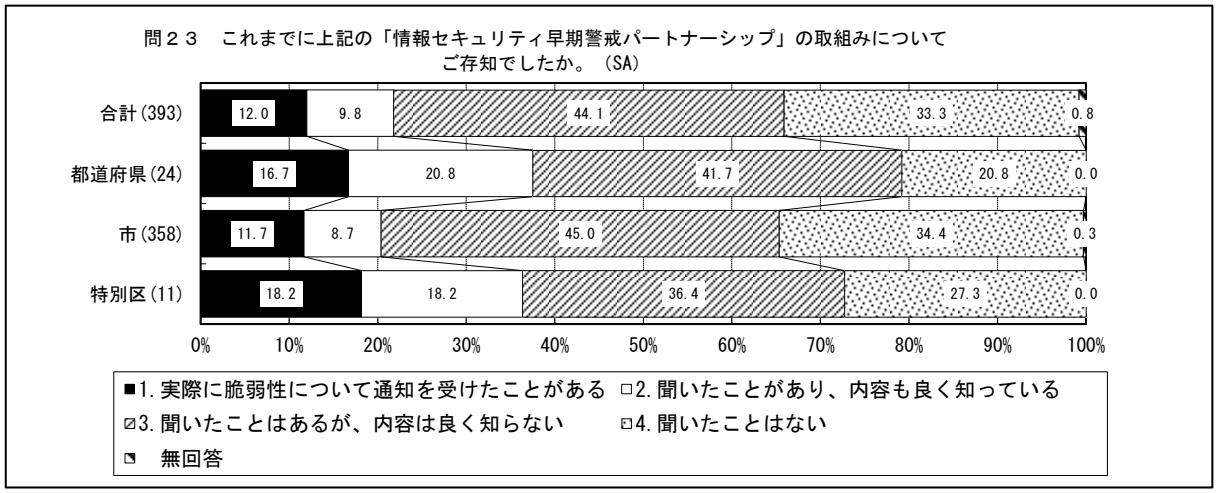

図 3.2-44　「情報セキュリティ早期警戒パートナーシップ」の取組みの認知度

3.3.ヒアリング対象とした地方公共団体の概要

ヒアリング調査は、アンケートの回答に基づき、8 件実施した。ヒアリング先を選定する上で基準としたアンケート項目は、『脆弱性対策を複数実施しているかどうか』(3.2.8小節)、『脆弱性検査や脆弱性診断サービス利用しているかどうか』(3.2.9小節)、『運用するサービスに脆弱性があるという情報を入手した際に公開するかどうか』(3.2.14小節)とした。内訳は、市が 5 件、都道府県が 2 件、特別区が 1 件とした。調査対象の規模(人口)の分布は表 3.3-1に示す通り。

表 3.3-1地方公共団体関係者に対するヒアリング先の人口規模

	区分			
人口	市	都道府県	特別区	総計
5～10 万人	2			2
10～20 万人	1			1
20～30 万人				0
30～40 万人				0
40～50 万人	1			1
50 万人以上	1	2	1	4
総計	5	2	1	8

表 3.3-2地方公共団体関係者に対するヒアリング先の抽出方針

タイプ分類	都道府県	区	市
脆弱性対策を複数実施しているケース	1	1	1
脆弱性対策を複数実施していないケース	1	-	1
脆弱性情報の公表について自治体の方針と合わないケース	-	-	3

3.4. ヒアリング結果の概要

3.4.1. 透明性、安全性、可用性のバランスについて

地方公共団体と脆弱性情報を共有する方式を探る上で重要な、情報公開ポリシー(透明性)と公表によるリスクのバランスについて地方公共団体のとらえ方を把握する。関係するアンケートの項目は3.2.14である。

回答の要点は以下の通り。

- 「公開が行政のあり方である」という意見もあり、未公表の脆弱性でも公開される可能性がある。その一方、「未公表の脆弱性情報は『公開により住民に被害の及ぶ可能性がある場合は非公開にして良い』という例外条項に該当する」という意見もある。また、サービスを停止する場合は、住民や議会に説明を求められることもある。
- 脆弱性を悪用した攻撃のリスクを判断する必要があり、その際には自治体の被害状況などの判断材料が必要である。
- サービスを停止する場合は、住民や議会に説明を求められることもある。

表 3.4-1　透明性、安全性、可用性のバランスについて

地方公共団体	アンケート回答における脆弱性情報の扱い	脆弱性を攻撃された被害経験	ヒアリング結果(安全性、透明性、可用性の優先順位、判断基準)	ヒアリング結果（コメント）
A市	住民への公表は控えるが、システムは稼働し続ける	なし	可用性 (重要なデータの有無)	・より多くの重要なデータがあるのであれば、対応が変わってくる。 ・ **特に脆弱性対策と言わず**、サーバのメンテナンス枠でパッチを当てている。 ・ 条例に基づく公開原則はあるが、**公開により被害がある場合は例外として非公開にして良いという原則**に従う。
B県	住民への公表は控えるが、システムは稼働し続ける	なし	可用性	・当初から「脆弱性の問題は例外事項に該当」と判断に基づき扱っている。 ・情報セキュリティポリシーには、ネットワークの運用という観点から脆弱性の扱いについて規定している。

C県	状況次第	なし	安全性、可用性	・ **住民への影響が出てくる場合は、情報公開条例の例外に定める非公開に該当**するものと判断。 ・何の対策も打たずに公開ということはできないだろう。しかし、脆弱性のある状態で動作させ続けて攻撃があると問題となる。攻撃された形跡があるのであれば、その被害も精査しなければならない。 ・自治体としてはサービスを提供している以上、住民に影響がでないようにする必要がある。止めることの影響と、止めないことのリスクの判断になってくる。まずは安全性と可用性のバランスがあって、その上で止めるという判断をしたときに説明しなければならない。**止める場合には、止める理由をある程度説明する必要がある。**
D市	住民に公表するが、システムは稼働を継続	なし	可用性 (事例、判断基準が無い)	・ 時々の事象に応じて、上司と相談するだろう。今までこういう事象が無かった。 ・ Web サイトを止めることは無いと思うが、公表するしないの判断がある。 ・ 脆弱性のレベルにもよると思う。**全国的に被害が出ているとわかっている時に稼働し続けるのも問題**である。
E市	住民への公表は控え、システムは停止	なし	安全性 (システムの停止は、事件事故が起きた場合であり、攻撃を受けていない段階での判断基準はない)	・ 脆弱性を公表する際には、社会的信用の失墜などを判断しなければならないが、そのための**判断情報が必要**となる。 ・ **意図的に自治体が狙われているのか、攻撃の傾向、攻撃の頻度、などという情報を得られれば**判断は付きやすい。 ・ 脆弱性情報については、発信元の方で開示範囲制限をしている場合もある。
F区	住民に公表し、システムは停止	あり	安全性 (サイトの規模による。今までは住民に対して具体的には公表していない)	・ 障害が発生したときには、止めずに代替サイトに切り替える。**原課としては、問題があるから止めると公表することを嫌がる**。 ・ ホームページを停止する際には住民、職員、議員に**説明をしないと止められない**。 ・上司に危険があるが稼働して良いかという判断を仰がなければいけないが、脆弱性の具体的状況やそのリスクを理解してもらうのは、上にいくほど難しい面がある。
G市	住民に公表するが、システムは稼働を継続	なし	安全性 (基準はない)	・情報を公開しているのが行政のあり方だと思い回答した。ルールづけられているわけではない。
H市	住民に公表するが、システムは稼働を継続	なし	透明性、可用性	・ 脅威の内容による。アクセスだけで危険であれば止めるしかない。 ・ 情報は丸めて公開する。対策中、障害があり、脅威がある、くらい。

3.4.2.啓発対象と内容、および効果的な普及策について

地方公共団体に対して脆弱性対策を啓発する際に、提供対象とするべき層とその内容、および効果的な普及策に関しては以下のような意見であった。

- 経営層管理層
  - 被害事例における被害額を地方公共団体の予算と関連づけて示す。(A 市,D 市,E 市)
  - 脆弱性の対策を怠って被害が発生した場合、結果的に市民からの信頼を失う恐れがあることを示す。(E 市)
  - テレビや新聞で報道されている事例について示す。(A 市,B 県)
  - 統計情報を継続的に提示する（例：周辺都市におけるツールの導入状況）(D 市,E 市)
- オーナー部門（原課）
  - 原課における脆弱性対策の方法について示す(C 県,G 市)
  - IT 担当部門による支援の必要性について、マニュアル・ガイドラインの形で示す。(C 県)
  - 委託先への注意喚起も重要であるということを示す。(F 区)
- IT 担当部門
  - IT 担当部門が脆弱性の情報をうまく裁けるような体制管理に関する資料を示す。(C 県)
  - どういう手法で、どこが狙われているかといった差し迫った情報を示す。(C 県)

表 3.4-2　啓発資料の対象と内容について

啓発資料の対象	内容
経営層・予算管理部門	[A 市] ・予算取りに使う資料には、被害状況の資料があると良い。対策を怠った際に起こる悪いケースの資料があると良い。 ・衆議院のメールサーバの話など、関心のある資料が良い。 [B 県] ・現場に近い人向けよりは、上の人向けの資料がよい。上に上げていくときにひっかかることがあるため。**「動いているのならそれでいいのでは」と思ってしまう人もいる**ので思わぬ落とし穴がありますよ、ということを伝えられれば良い。 ・(情報セキュリティ関係の）ニュースが多いと、議員からの質問などで話題に上がることはある。**ニュースの内容の意味はよくわかっていないが、どういう影響があるのか、**などの情報には関心がある。 [D 市] ・金銭的な面からの指摘が良い。例えば損害賠償の事例が挙げられる。事例における**損害賠償と市の予算**との関係も良いだろう。 ・ツールを分類して、同じくらいの規模の市がどれくらい導入しているか。対策の遅れを示せる。 [E 市] **・定期的な情報提供をして欲しい**。啓発は継続的にやらないと忘れる。 **・対策を怠った際に**生じる被害について。**『市民からの信頼を失う』**、ということが伝われば良いだろう。 ・防衛産業での情報セキュリティ関係の事件・事故は興味があるだろう。
オーナー部門（原課）	[A 市] ・研修などでも映像を伴うと反応が良い。 [C 県] **・各原課での対応と IT 担当部門による支援の必要性**を記載したマニュアル・ガイドライン

	[F 区] ・IT 担当部門以外で管理している原課や外郭団体にわかるような資料が良い。**委託先への注意喚起**も重要であるということを伝えて欲しい。 [G 市] ・原課は、委託先に脆弱性対策を丸投げとなりかねないので、脆弱性対策の意識を持たせるようにしてほしい。
IT 担当部門	[C 県] ・IT 担当部門が脆弱性の情報をうまく裁けるような**体制管理**に関する資料が良い。 **・各原課での対応と IT 部門による支援の必要性**を記載したマニュアル・ガイドラインが良い。 [E 市] ・IT 担当部門には、どういう手法で、どこが狙われているかといった、差し迫った情報があれば良い。 [H 市] ・業者がやっていることをどう確認するか、といったノウハウ。IT コーディネーターの活用などが例として挙げられる。
その他	[D 市] ・事件の情報を伝え、議員からの質問が出ると対策をする必要が認識される **・被害実態調査などの統計情報は継続的に提供**してほしい

表 3.4-3　啓発資料の配付方法について

啓発資料の配布方法について	
都道府県により開催される地域の勉強会	市区町村の IT 担当が集まる勉強会
IT 担当課	直接送付
LASDEC の ML	「お知らせ」として送付

3.4.3. 地方公共団体が認識している課題について

地方公共団体が、現在認識している課題について表 3.4-4に示す。『脆弱性対策の予算確保』について課題とした地方公共団体が 50%の 4 県あった。

表 3.4-4　地方公共団体において現在認識されている課題について

課題	**組織**	**ヒアリング結果**
人材育成・確保	A 市	・人事異動が定期的にあるので、3 年目から異動対象になる。やっと使えるようになった時に異動になってしまう。最低でも 5 年は配属させてほしい、と申請してはいる。 ・人材育成が難しい。研修のカリキュラムが整備されていないので、整備していきたい。
	H 市	・研修等をやっても現場で無いと分からないことが多い。庁内的な事務と IT 関係の業務であり、業者と話ができるまでに３年はかかる。5 年超えないと工事などにも対応できない。
脆弱性対策の予算確保	A 市	・脆弱性で予算を確保するのは難しい。今すぐでないといけないのか、といわれてしまうと難しい。緊急にやらないと明日明後日に止まるとわかっていれば対処できる方法もあるだろうが。
	B 県	・突発的な脆弱性対応も含めた委託費用になっているので、費用が高い。
	E 市	・新たな技術を取り入れて自動化などを進めて行きたいと考えているが予算が手当されない。予算、人手が不足している。
	G 市	・保守業者がパッチあてして、システムが正常に稼働するかチェックするための工数が発生する。その検証費用が今後増えるのではないかと懸念している。

経営層・予算管理部門の脆弱性対策	E 市	・上層部は脆弱性の意識が希薄になりがちである。うまく浸透しないというところも感じている。
原課の脆弱性対策	C 県	・システムを所管している原課に IT 担当課から情報を提供する。原課が判断、委託業者に照会、その後対応、というのが実情だろう。本来ならば、IT 担当課で、システムごとに割り振れれば良いが、脆弱性と各システムの詳細まで知識がないとわからない。 ・本来 IT 担当課で把握したいが、原課まかせになっている状況である。実際、今の体制で原課の状況を把握するのは厳しい。 ・LASDEC の今年の検査について、原課にいかにうまく登録してもらうかを考えている。
	G 市	原課は、業務が効率的にできることを中心に考えるので、脆弱性対策まで気が回りにくいというところもあり、ベンダー任せになりやすい。
原課との関係	D 市	・原課の保有するシステムの構成、ソフトウェアのバージョンについて、例えば、この OS を使っている、と台帳管理してきたが、大変になってきたので、自動的に管理できる資産管理の仕組みを来年度から作って活用してきたい。
	E 市	・原課に脆弱性の情報を連絡しても関係ないと言われることもしばしばある
指定管理先・外郭団体の管理	C 県	・県のウェブサイトではなく、指定管理先のウェブサイトが攻撃された。公営競技場など県立の施設は、指定管理で丸々運営を委託している。
	F 区	・外郭団体を管理する所管が 10 数カ所あり、それぞれ HP を持っている。所管から手を出しにくい。
委託業者の脆弱性対策、納品物の検査	F 区	・脆弱性を、委託業者が直してくれたかどうかの検査が大変である。職員が検査員になってといわれても能力的にできない。どこかに頼んで検査するような仕組みが必要ではないか。 ・納品されたものを検査する仕組みが必要だろう。
	H 市	・業者がやっていることをどう確認するか。業者がやった手順を説明させて確認させることではないか。
その他	A 市	・脆弱性があって困るのはオープンソースソフトウェアだと思う。Apache を使っていて不具合があった問いに相談できる窓口があると良いと思う。
	G 市	・直面している課題は無いという認識でいるが、国の機関で起きている標的型攻撃まで考えると課題として認識する部分もある。 ・IPA から注意喚起があり、入口対策と出口対策を、と言われた。現実的に出口対策としてどのような手を打てるのか。セキュリティソフトメーカーに来てもらったりもして情報を集めているが、経費が課題である。

4. 考察

4.1.「脆弱性情報に関する透明性、安全性、可用性の判断」の選択理由の分析

4.1.1.「脆弱性情報に関する透明性、安全性、可用性の判断」の現状と、ウェブサイト関連システムに脆弱性対策を進める上での課題認識との関係について

- 便宜上、図 4.1-1 の 4 つの選択肢を以下のように呼ぶこととする。

  『1.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知するが、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ』
  → 『1.周知・サービス維持』

  『2.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知し、当該システムは安全のため対策完了までは停止する』 → 『2.周知・サービス停止』

  『3.攻撃を受けるリスクを抑えるために脆弱性の存在については対策を適用するまで住民への公表を控え、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ』 → 『3.非公表・サービス維持』

  『4.攻撃を受けるリスクを抑えるために脆弱性の存在については対策を適用するまで住民への公表を控え、当該システムは安全のため対策完了までは停止する』
  → 『4.非公表・サービス停止』

- 運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応（3.2.14）として、『1.周知・サービス維持』は 5.0%が選択した（図 4.1-1）。この場合、対策が適用される前に公表すると、システムが攻撃され住民の情報が流出するなどの被害が生じるリスクや他組織の類似システムが攻撃対象となるリスクがあるが、回答者がそれらのリスクを認識していない可能性がある。
- 『2.周知・サービス停止』については、35.1%が選択した（図 4.1-1）。この場合、他組織の類似システムが攻撃対象となるリスクがあるが、回答者がそのリスクを認識していない可能性がある。
- ウェブサイト関連システムに脆弱性対策を進める上での課題(3.2.22)のうち、『e.知りえた脆弱性等のシステムのセキュリティに関する情報について、秘密にすべきか、住民や企業への透明性を重視して公開すべきかが悩ましい』ことを『1.重要な課題である』と回答した地方公共団体については、『4.非公表・サービス停止』を選択する割合が 18.6%と、全体の 13%に比べて若干高い。
- ウェブサイト関連システムに脆弱性対策を進める上での課題(3.2.22)のうち、『f. 脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい』ことを『1.重要な課題である』と回答した地方公共団体については、『2.周知・サービス停止』を選択する割合が 40.2%と、全体の 35.3%に比べ若干高い。

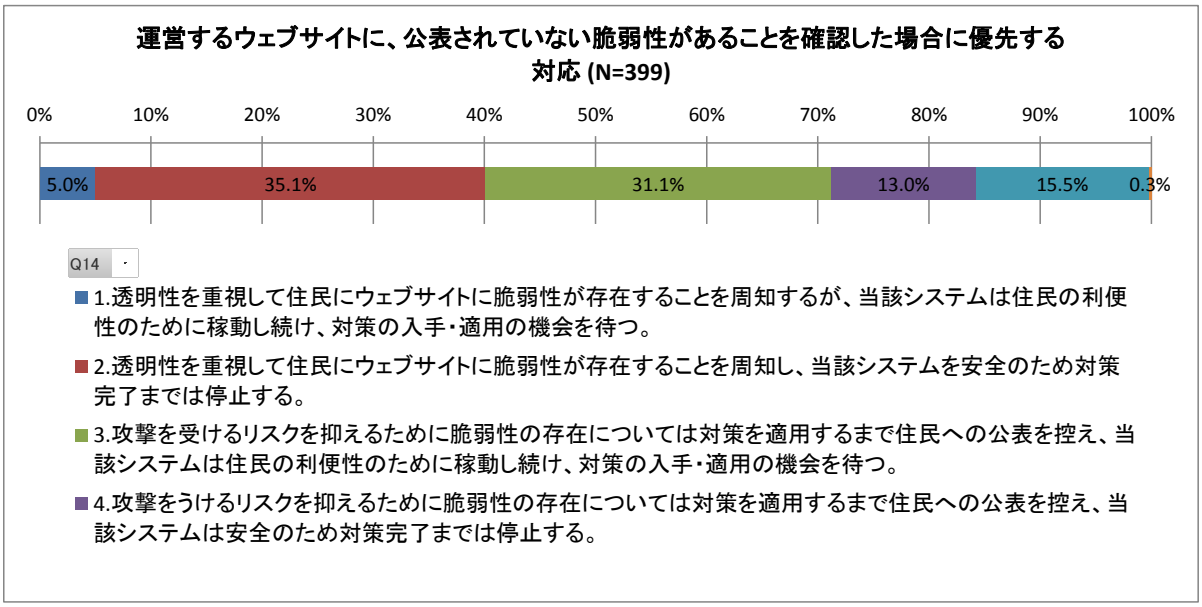

図 4.1-1　運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応

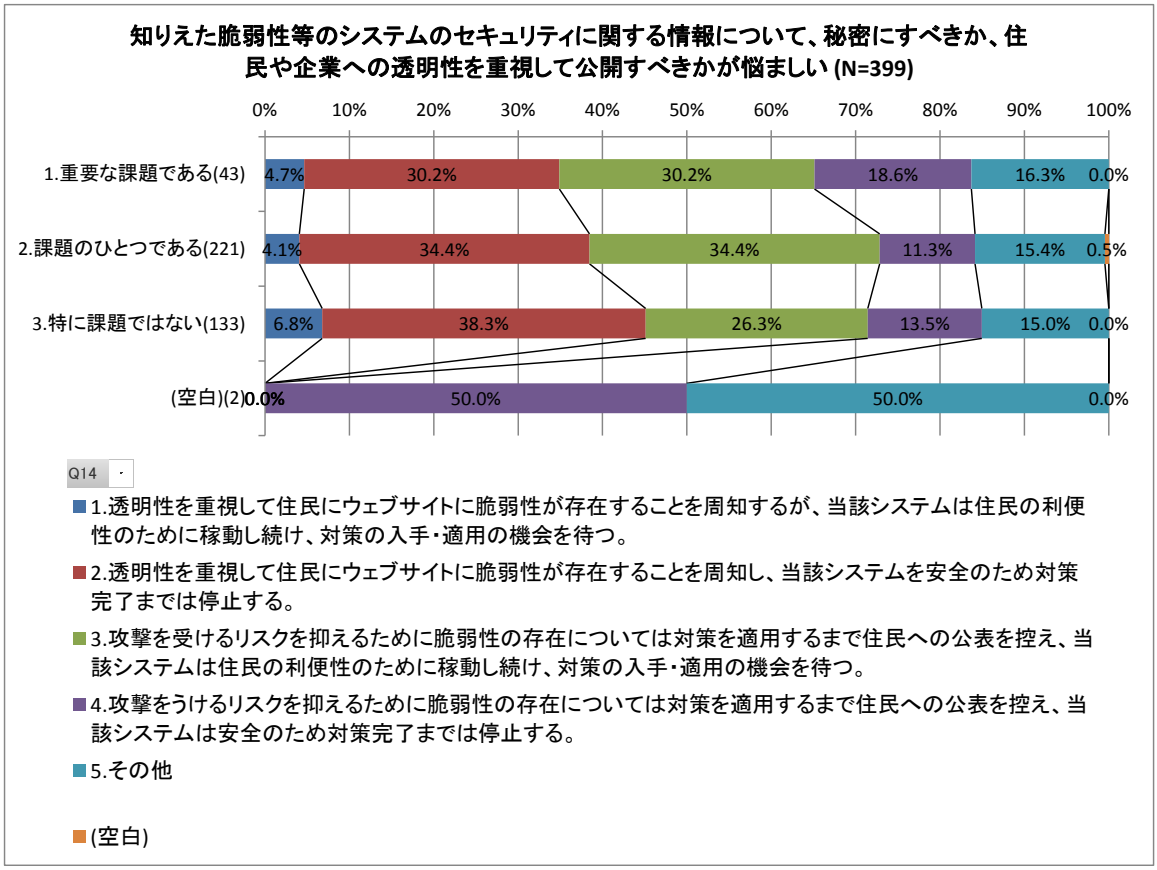

図 4.1-2　『知りえた脆弱性等のシステムのセキュリティに関する情報について、秘密にすべきか、住民や企業への透明性を重視して公開すべきかが悩ましい』ことの認識と『運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応』の関係

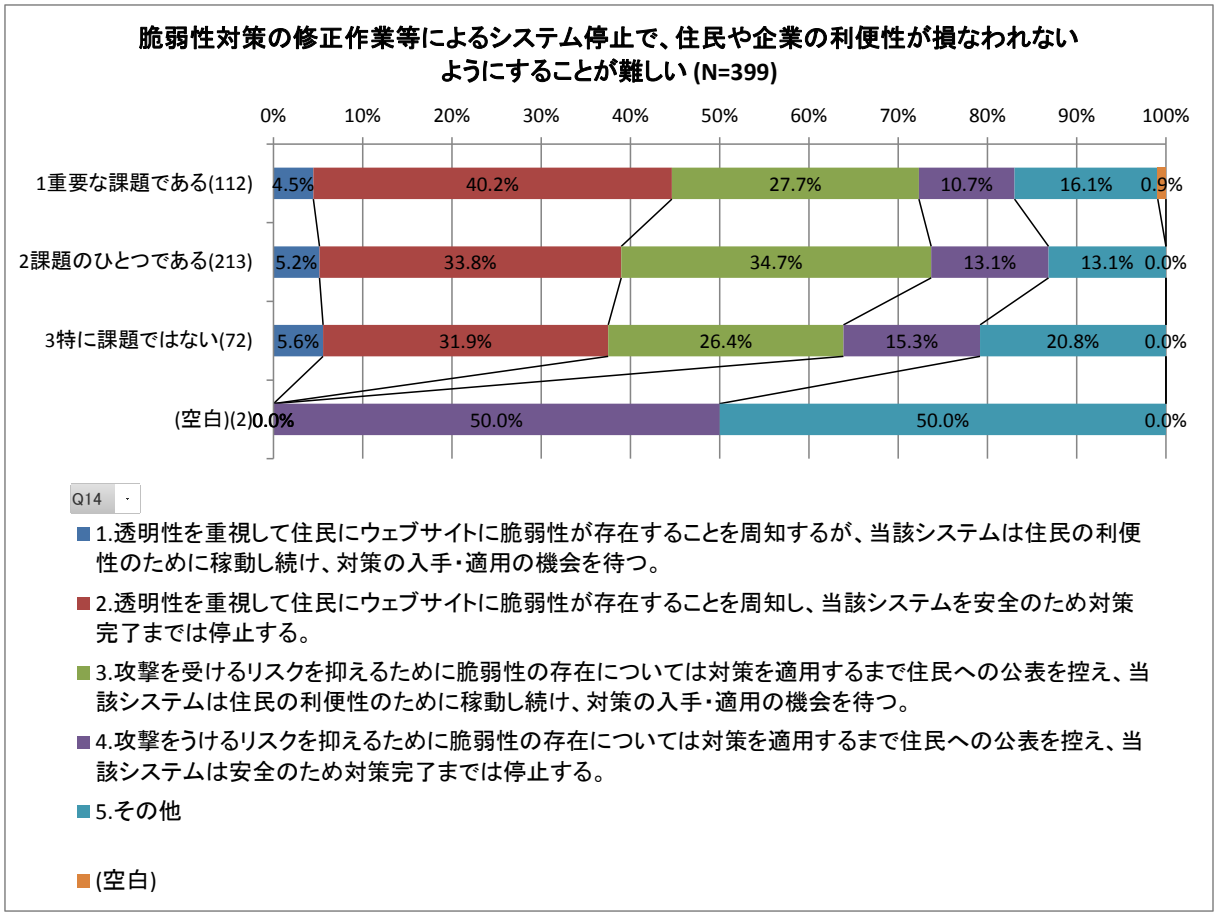

図 4.1-3 『脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい』ことの認識と『運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応』の関係

4.1.2. 「情報セキュリティ早期警戒パートナーシップに対する認識」の影響

・ ウェブサイトに脆弱性を発見した際に、情報セキュリティ早期警戒パートナーシップにより、『1. 実際に脆弱性について通知を受けたことがある』組織は 43.8%(21 件)が『3. 攻撃を受けるリスクを抑えるために脆弱性の存在については対策を適用するまで住民への公表を控え、当該システムは住民の利便性のために稼動し続け、対策の入手・適用の機会を待つ』としており(図 4.1-4)、同選択肢を選ぶ全体の平均値(31.1%)より高い(図 4.1-5)。これは、通知を受けた経験者の方がより客観的に脆弱性のリスクやサービス維持の必要性を判断したためと考えられる。

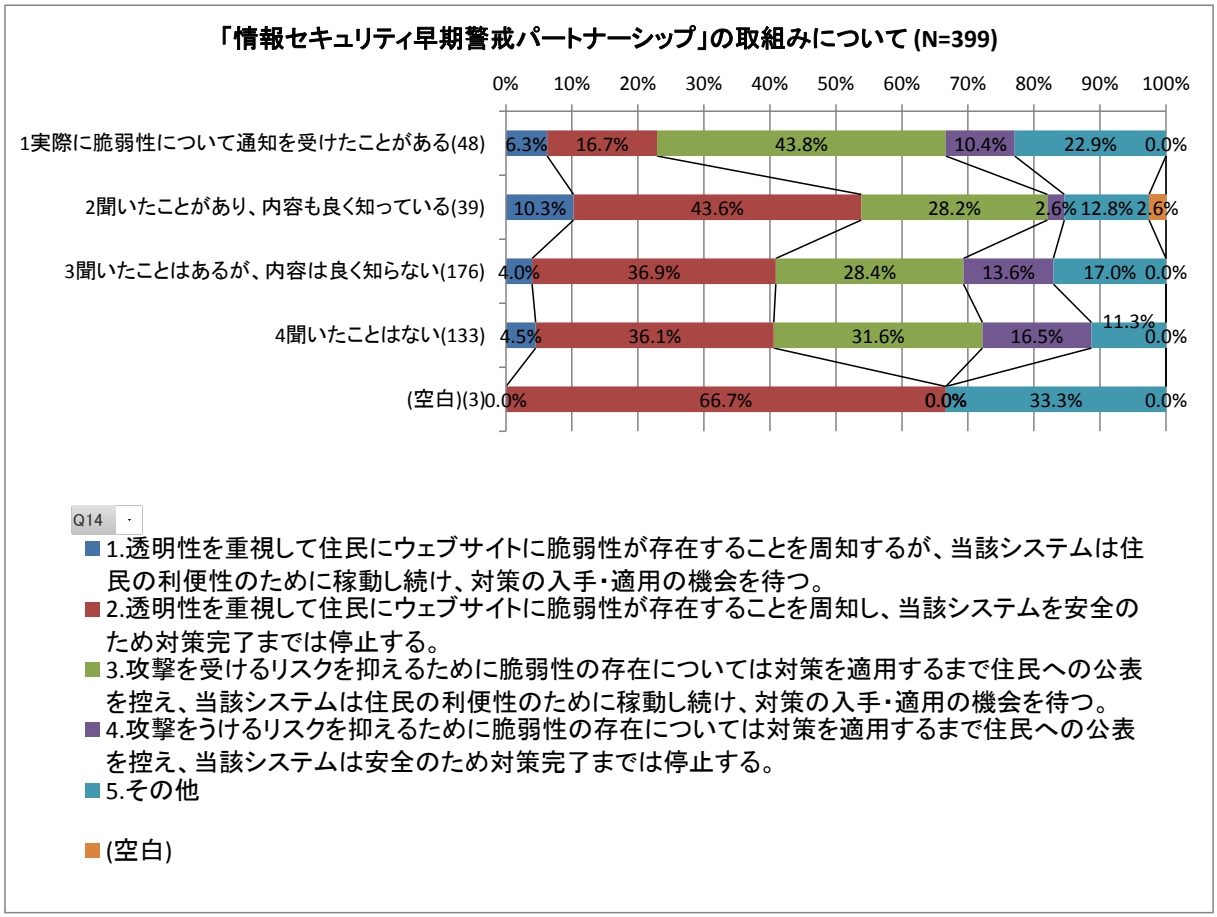

図 4.1-4 パートナーシップに対する認識と Web サイトに脆弱性を発見した際の対応の関係

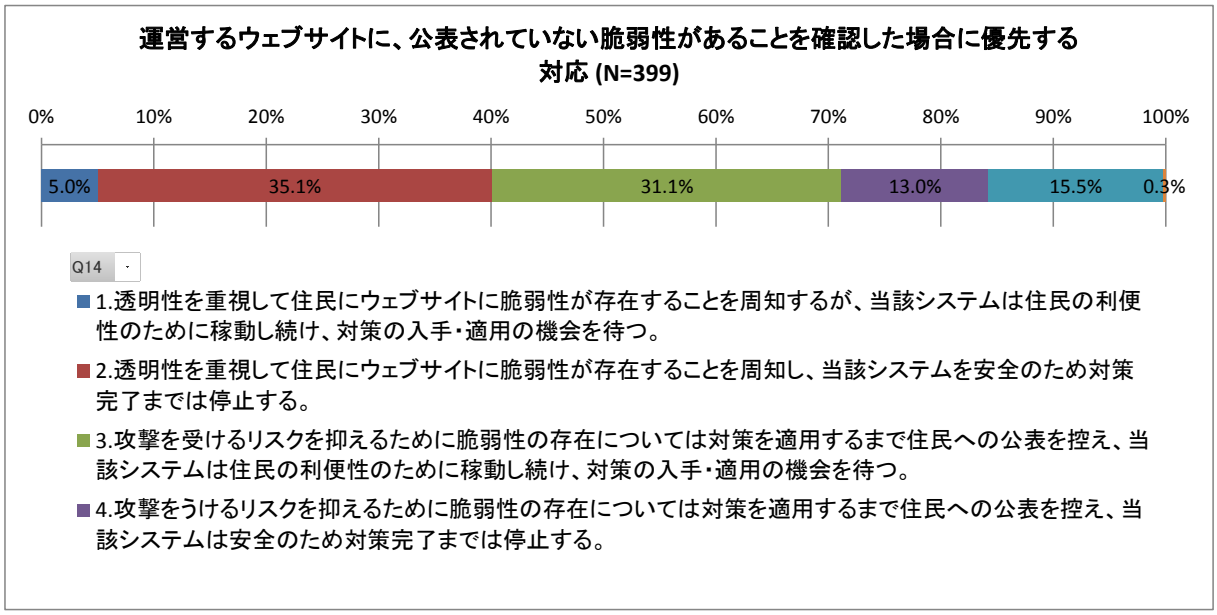

図 4.1-5 （再掲）運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応

・　しかし、8 割近くの地方公共団体からは十分に認識されておらず、同パートナーシップの普及啓発を継続することが求められる（図 4.1-6）。
・　市の中でも、人口が少ない市の方がより認識度の低い傾向にある（図 4.1-7）。

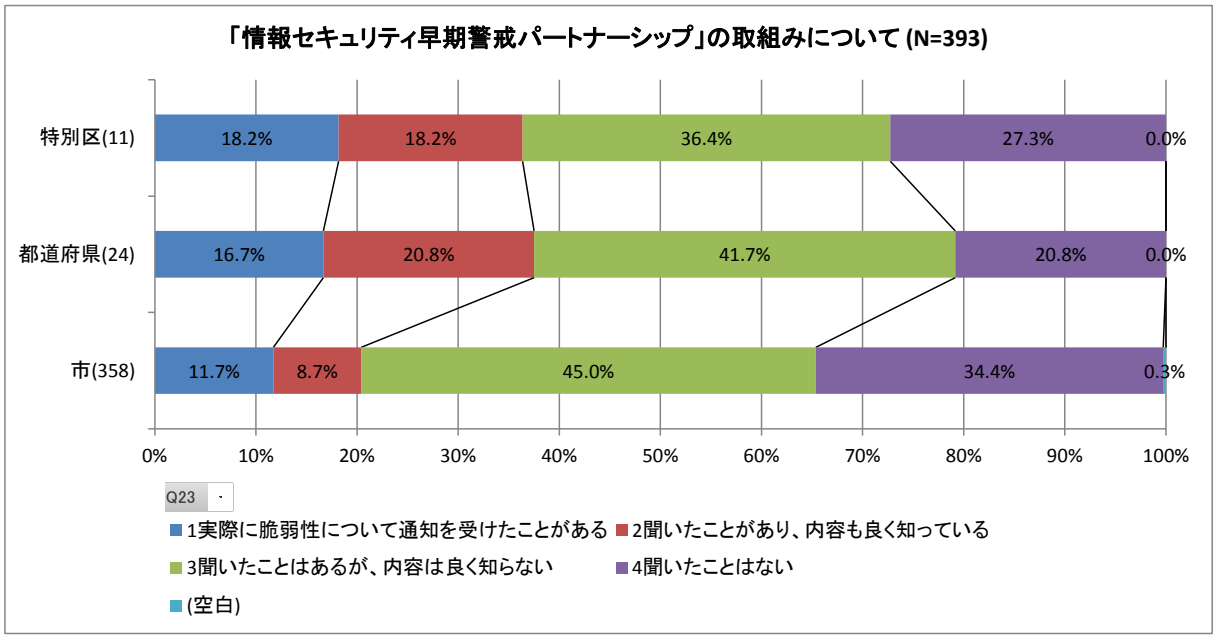

図 4.1-6　情報セキュリティ早期警戒パートナーシップの取り組みについての認識度

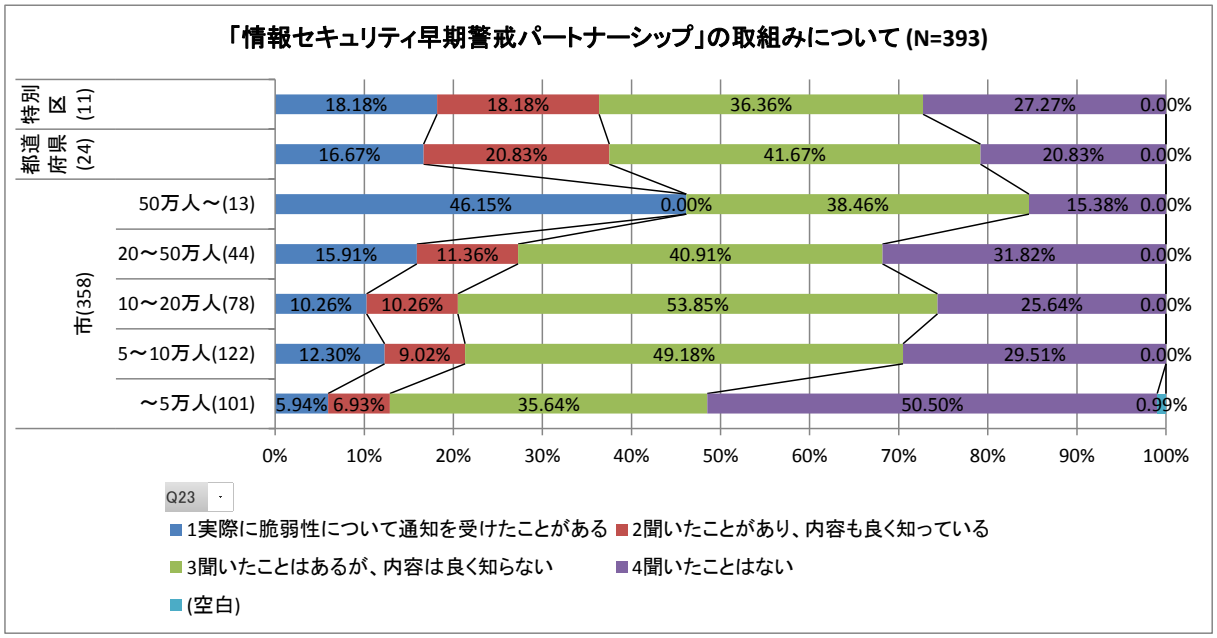

図 4.1-7　情報セキュリティ早期警戒パートナーシップの取り組みについての認識度（市、人口別）

4.1.3. ウェブサイトの脆弱性対策の適用の判断が遅れたり誤ったりしたため、ワームや不正アクセス等の被害に遭った経験の有無の影響

- ウェブサイトの脆弱性対策の適用の判断が遅れたり誤ったりしたため、ワームや不正アクセス等の被害に遭った経験(3.2.17)の有無と、運営するウェブサイトに、公表されていない脆弱性があることを確認した場合に優先する対応の関係を図 4.1-8に示す。
- 被害経験のある地方公共団体は、『2.透明性を重視して住民にウェブサイトに脆弱性が存在することを周知し、当該システムを安全のため対策完了までは停止する。』を選ぶ割合が 43.4%と、全体の 35%よりも高くなっている。

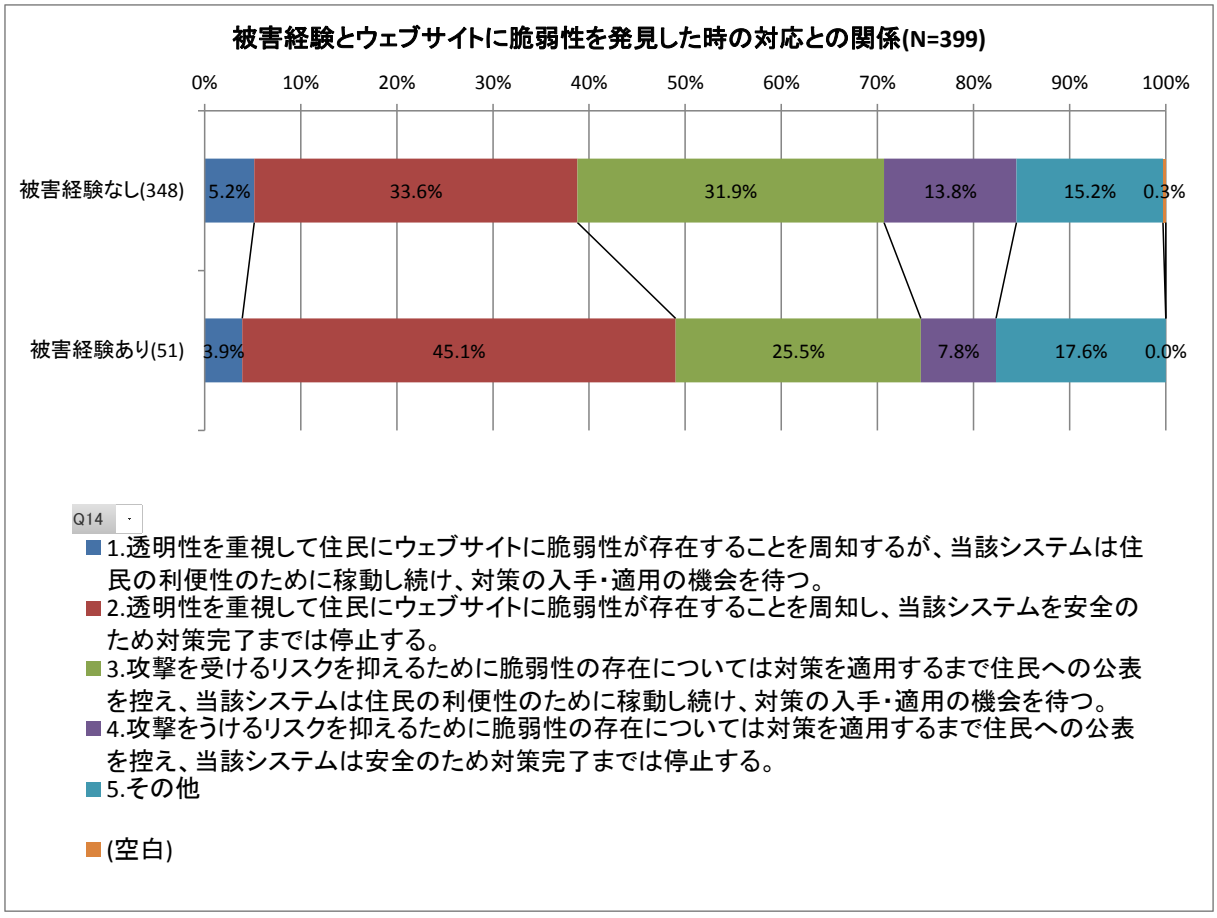

図 4.1-8　被害経験とウェブサイトに脆弱性を発見した時の対応との関係

4.2. 地方公共団体における脆弱性対策に係る課題

- 本調査のアンケートでは、ウェブサイト関連システムに脆弱性対策を進める上での課題について回答を得ている[8](図 4.2-1)。

[8] 3.2.22小節参照

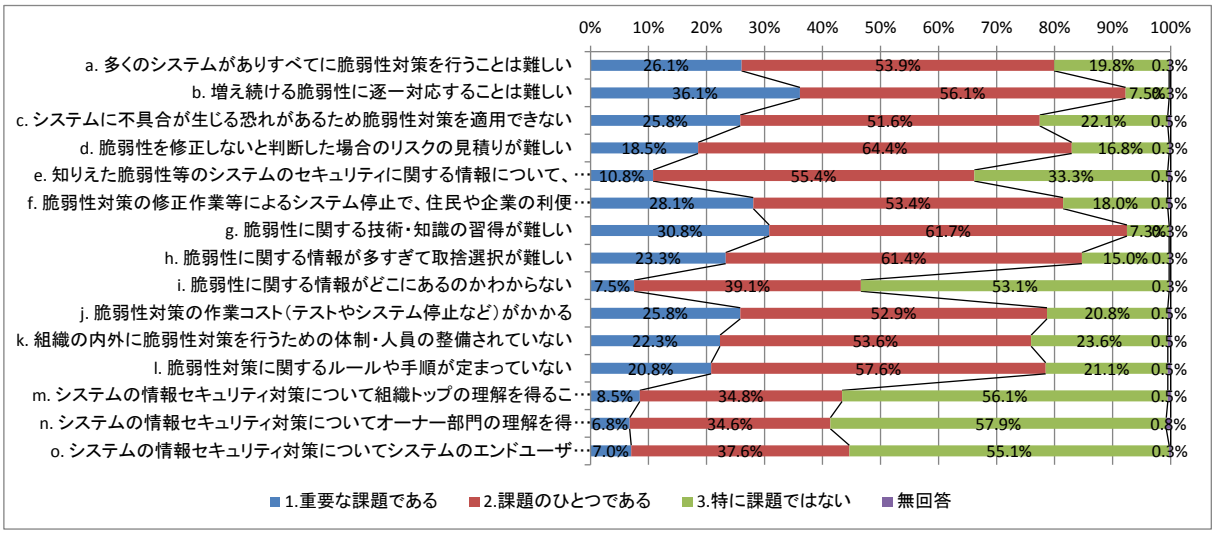

図 4.2-1　ウェブサイト関連システムに脆弱性対策を進める上での課題(N=399)

・　『住民』という言葉を含む、地方公共団体に特徴的な 2 つの設問、『知りえた脆弱性等のシステムのセキュリティに関する情報について、秘密にすべきか、住民や企業への透明性を重視して公開すべきかが悩ましい』(図 4.2-2)、『脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい』(図 4.2-3)について、特別区はそれぞれ 81.8%、100%が課題という意識を持っている。

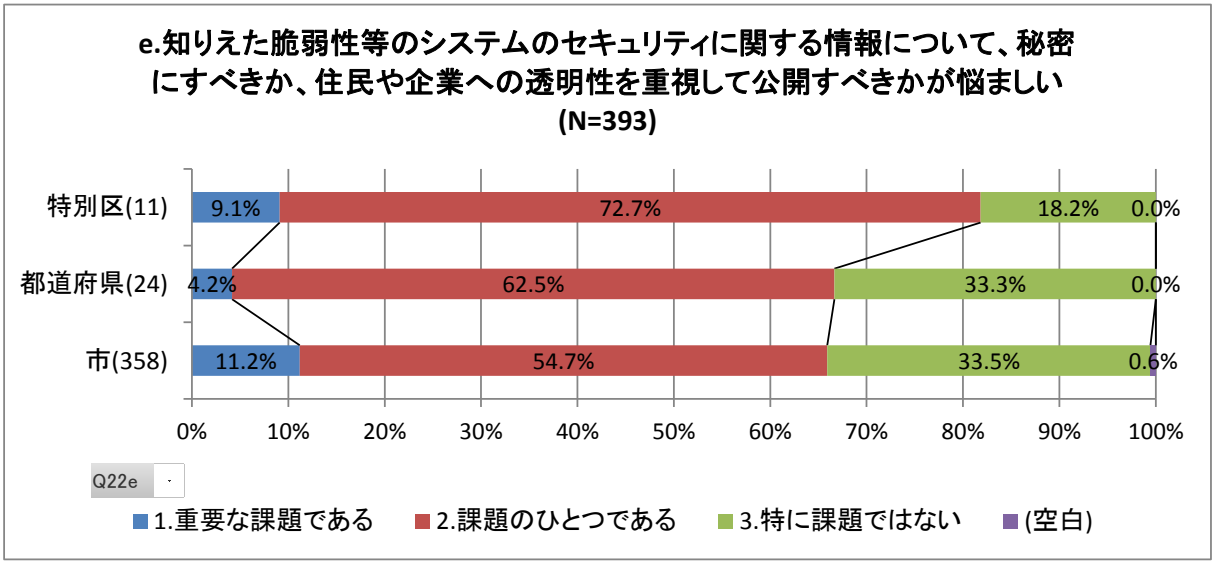

図 4.2-2『知りえた脆弱性等のシステムのセキュリティに関する情報について、秘密にすべきか、住民や企業への透明性を重視して公開すべきかが悩ましい』(自治体区分)

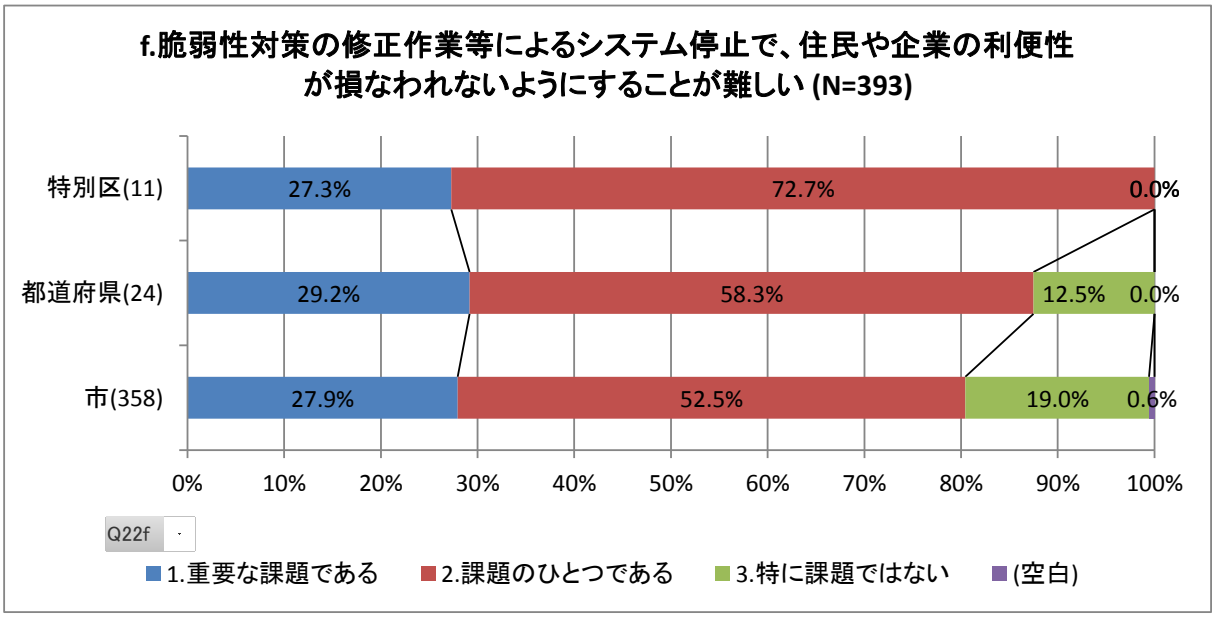

図 4.2-3『脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい』（自治体区分）

- 特別区の一部と人口の少ない市では、『m. システムの情報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』を『1. 重要な課題である』と回答する傾向にある（図 4.2-4）。
- 都道府県の一部と人口の少ない市では、『n. システムの情報セキュリティ対策についてオーナー部門の理解を得ることが難しい』を『1. 重要な課題である』と回答する傾向にある（図 4.2-5）。
- 特別区では、『o. システムの情報セキュリティ対策についてシステムのエンドユーザ（住民や企業）の理解を得ることが難しい』ことを 81.8%と高い割合で課題としている。

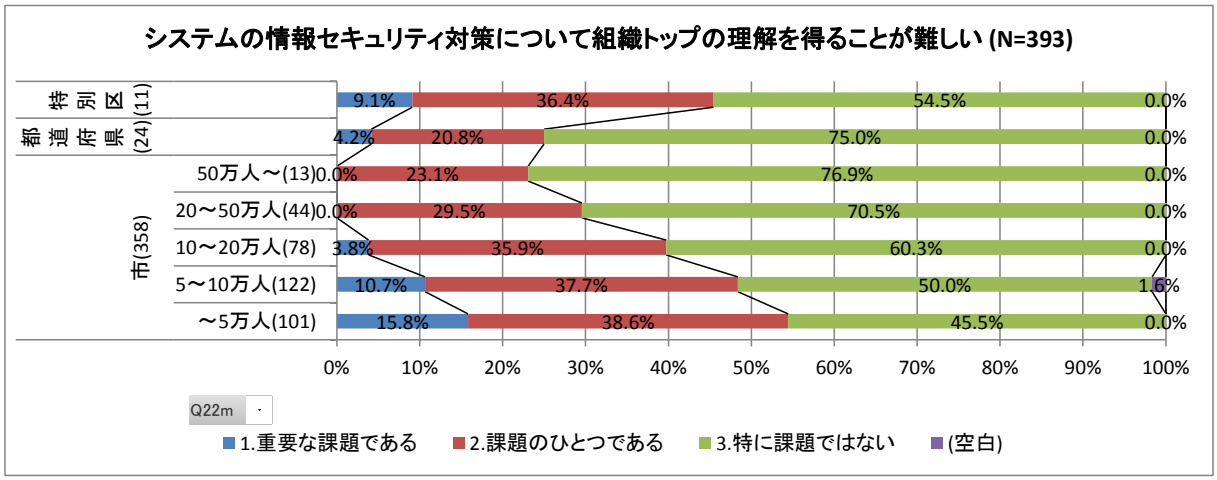

図 4.2-4　『システムの情報セキュリティ対策について組織トップの理解を得ることが難しい』（自治体区分別、市人口別）

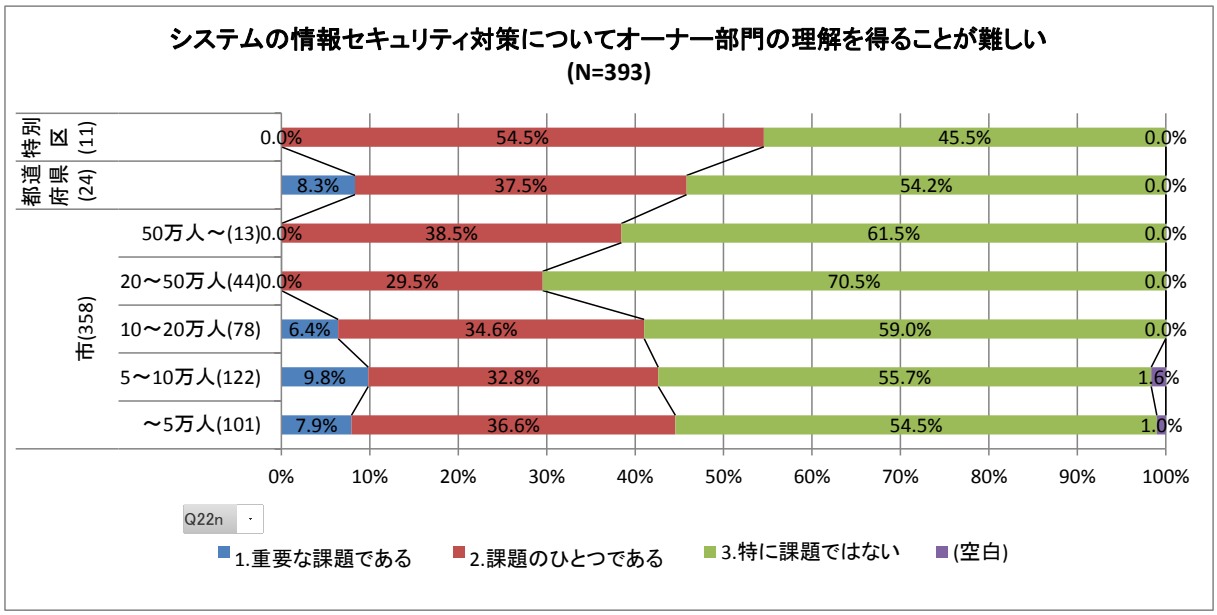

図 4.2-5 『システムの情報セキュリティ対策についてオーナー部門の理解を得ることが難しい』（自治体区分別、市人口別）

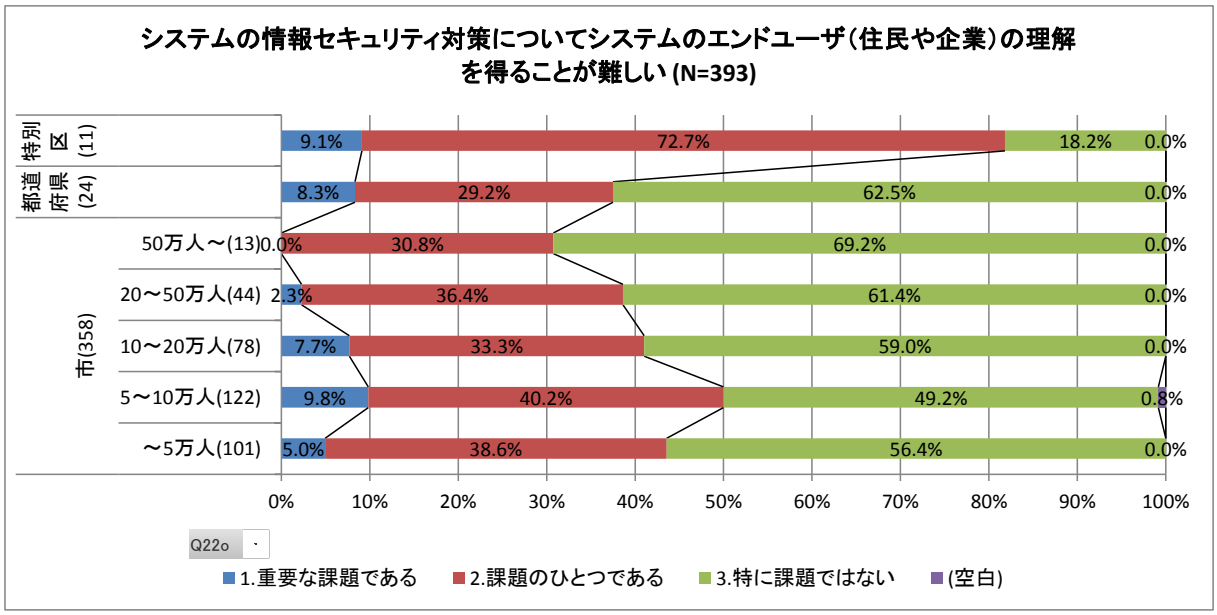

図 4.2-6 『システムの情報セキュリティ対策についてシステムのエンドユーザ（住民や企業）の理解を得ることが難しい』（自治体区分別、市人口別）

4.3. 人口を基準とした脆弱性対策の整備状況に対する分析

・ 地方公共団体において『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するか決めていない』、『運用中のウェブサイトについて、脆弱性検査や脆弱性診断サービスを利用

していない』、『脆弱性対策の一連の手順を文書化していない』ことと、人口の間には相関がある(図 4.3-1 図 4.3-2, 図 4.3-3)。

・ これには、人口の少ない市では人手や予算が不足していること(図 4.3-4)が原因と考えられる。ただし、市が情報システムを保有しないホスティング方式を選択した結果、脆弱性対策も委託業者がカバーしているケースも含まれている点に留意が必要である。

・ また、『運用中のウェブサイトの脆弱性対策に必要な費用』についても『3.脆弱性対策は委託先との契約に明記されていないが、事実上、委託費用に全て含まれている（個別の支払いはしていない)』を選択する地方公共団体は、人口と反比例する傾向が見られる。

・ これは、商慣行としては健全な状況にあるとは言い難いものであり、増加する脆弱性の状況を考慮すれば、委託先の負担はバランスを欠いたものになりかねない。今後、改善に向けた取り組みがなされることを期待する。

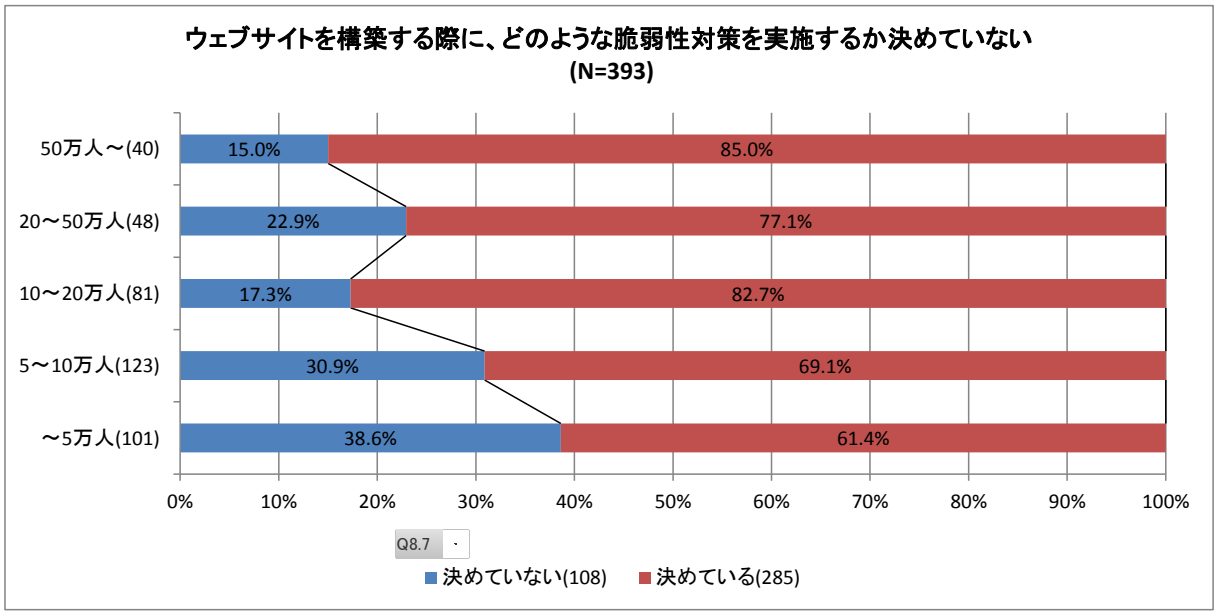

図 4.3-1 ウェブサイトを構築する際に、脆弱性対策の実施を決めているか（人口別）

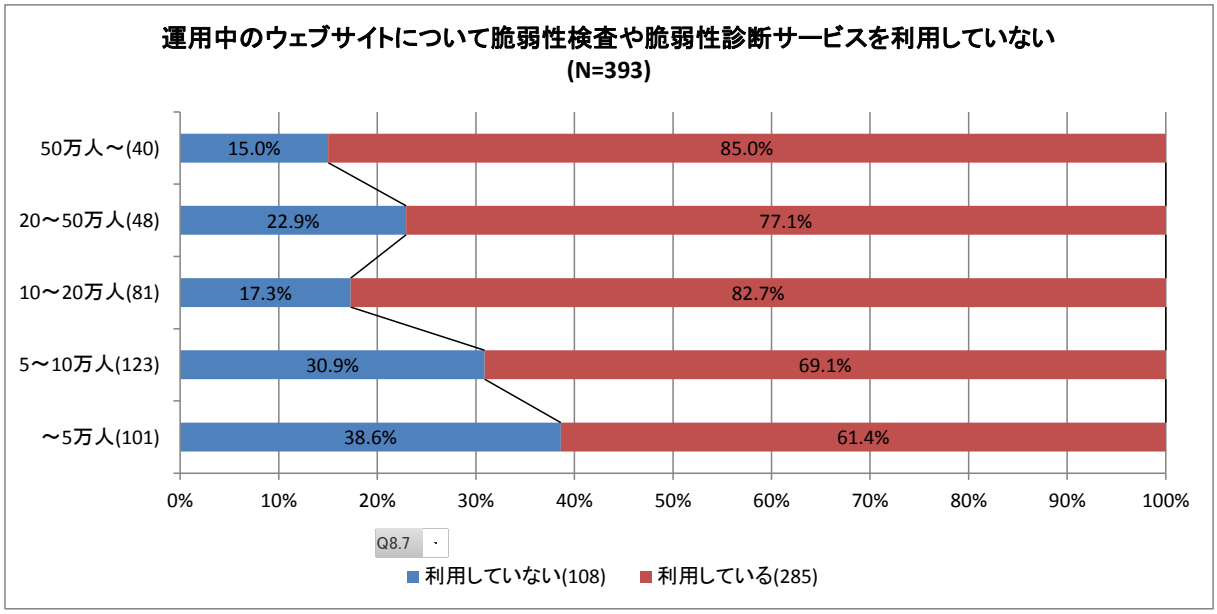

図 4.3-2　脆弱性検査、診断サービスの利用（人口別）

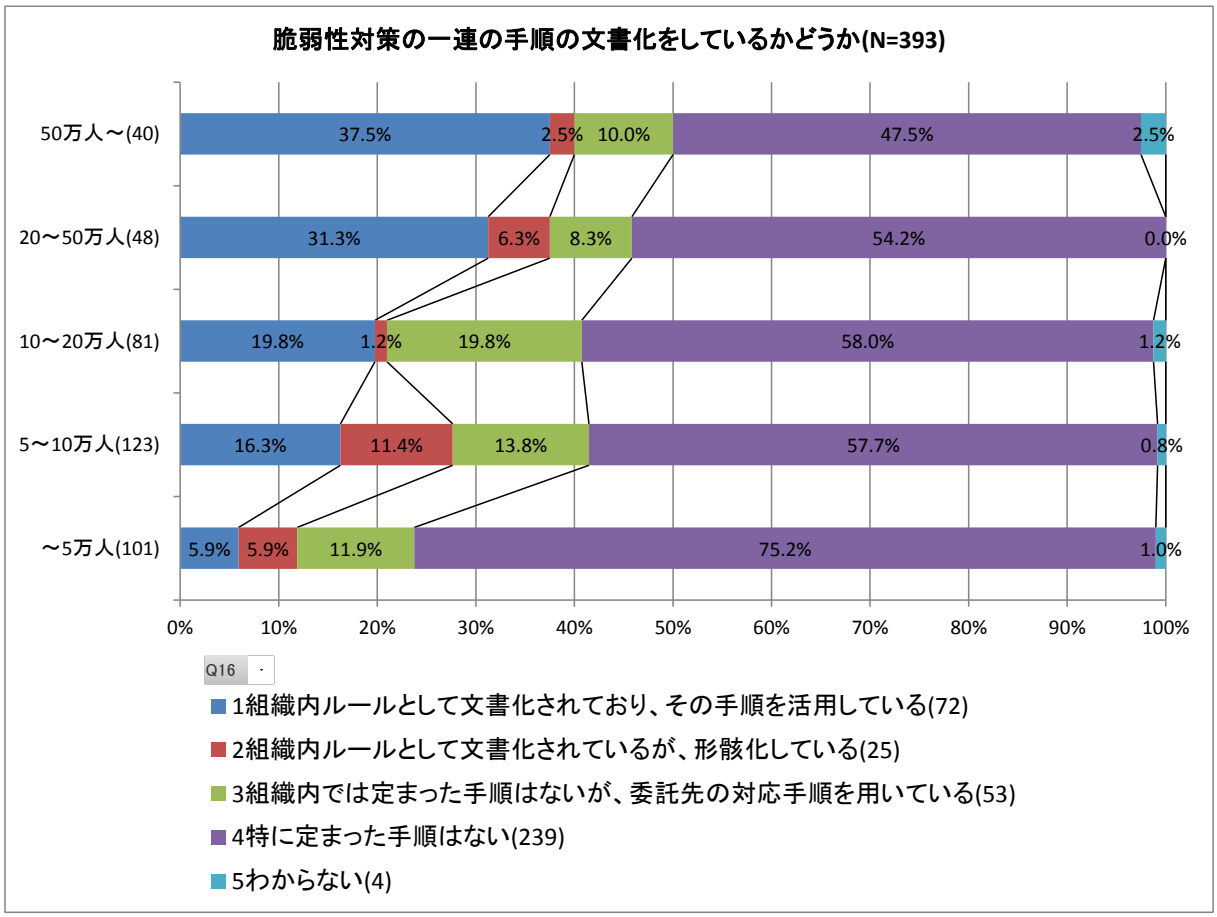

図 4.3-3　脆弱性対策の手順に係る文書化（人口別）

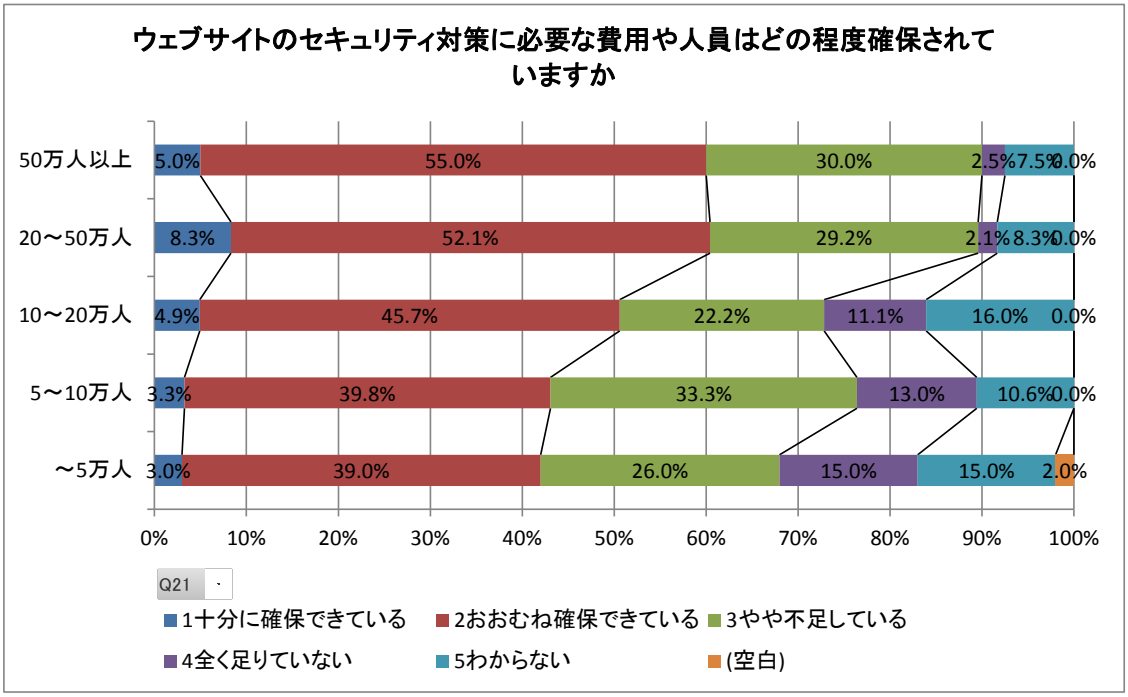

図 4.3-4　ウェブサイトのセキュリティに必要な費用と人員の確保（人口別）

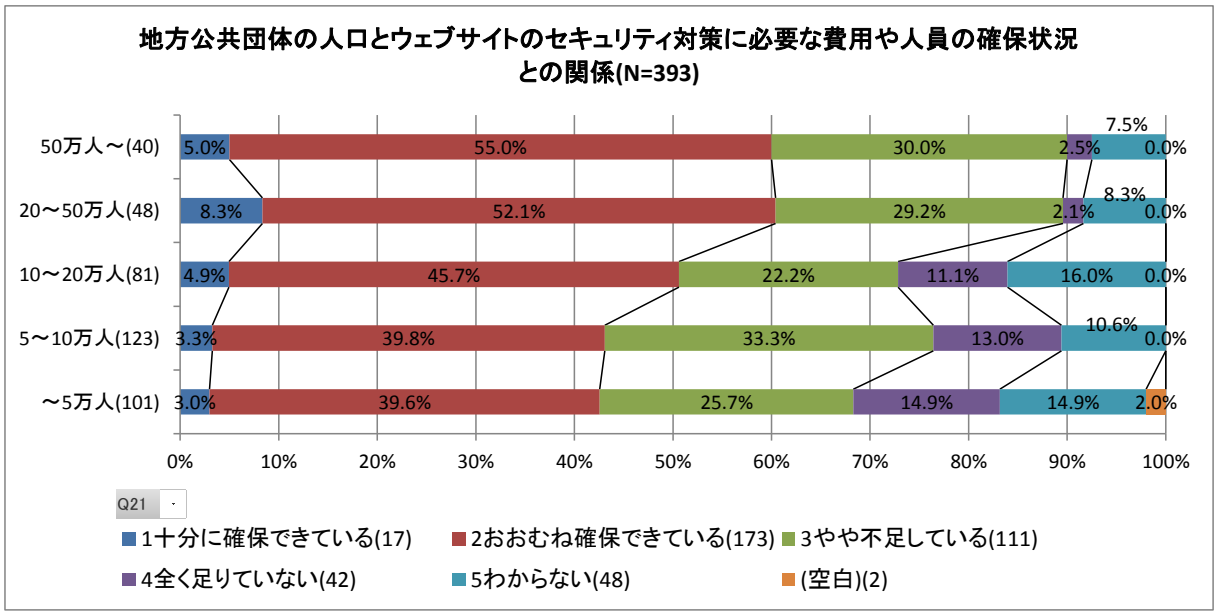

図 4.3-5　ウェブサイトのセキュリティ対策に必要な費用や人員の確保状況との関係（人口別）

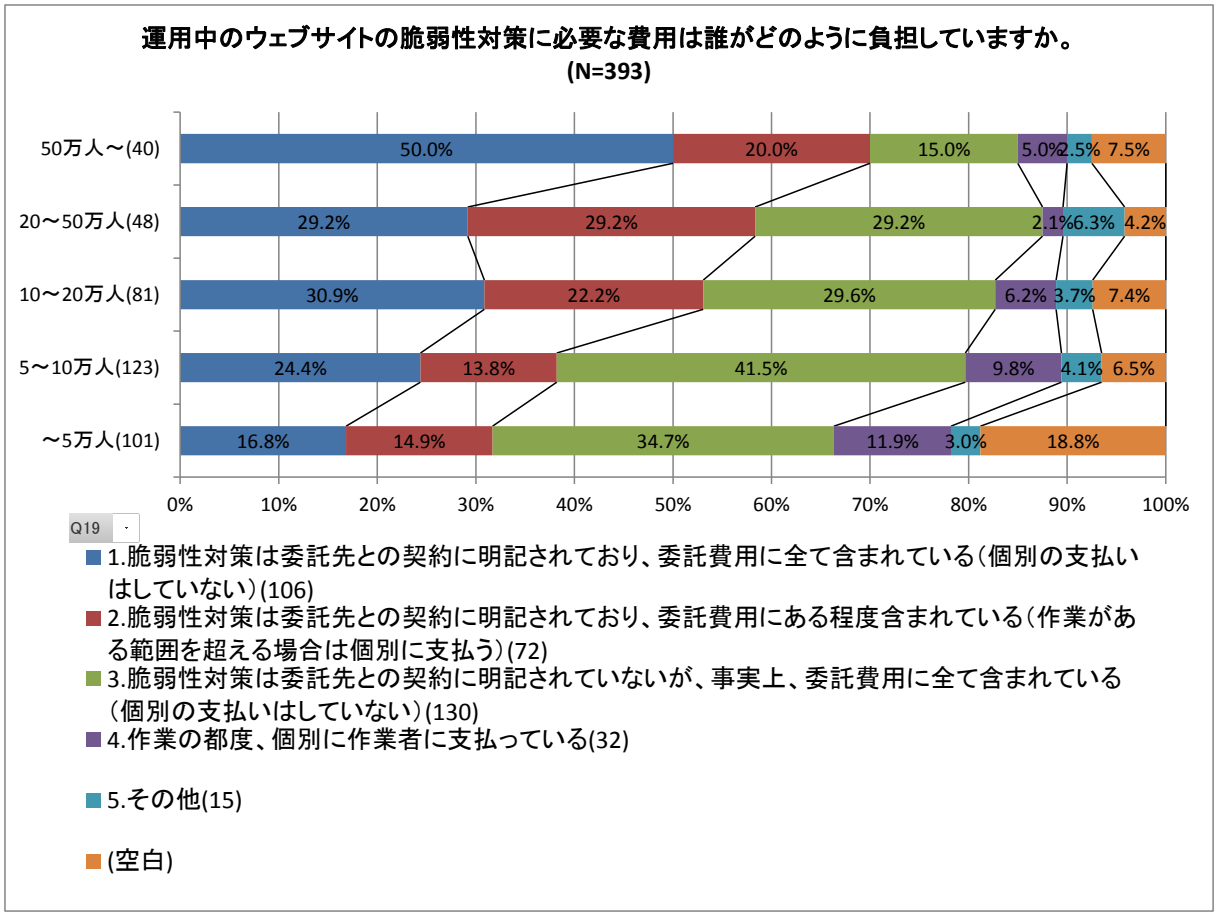

図 4.3-6　運用中のウェブサイトの脆弱性対策に必要な費用の負担（人口別）