資料 1-5

小規模ウェブサイト運営者の脆弱性対策に関する調査

1. 調査背景・検討概要

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

（1）アンケート調査

対象：小規模ウェブサイト運営者
有効回答数：300件以上

（2）アンケート結果の分析

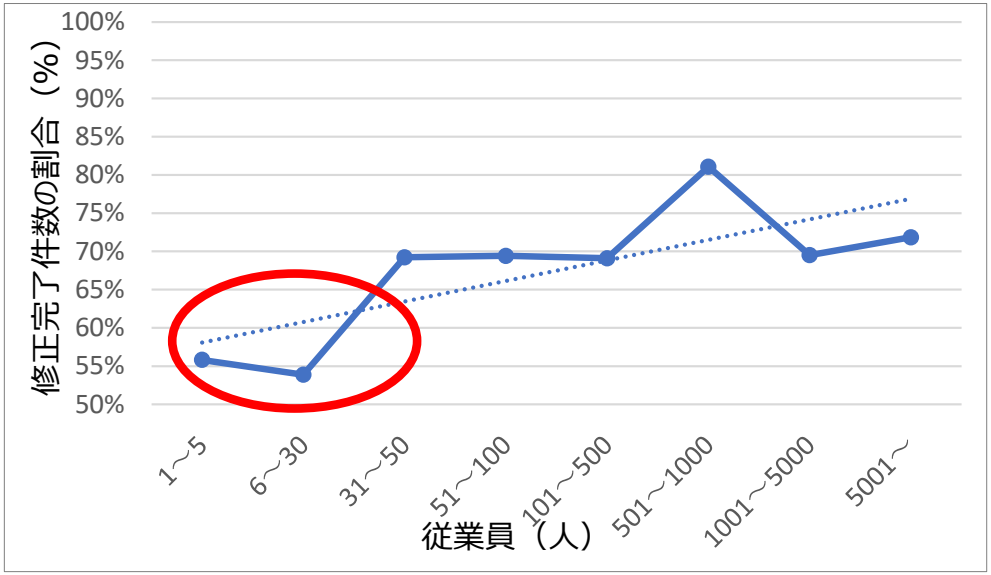
（3）「企業ウェブサイトのための脆弱性対応ガイド」の改訂の要否検討

- 改訂する場合は、改訂案を第2回の脆弱性研究会に提示

（アウトプット）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
「企業ウェブサイトのための脆弱性対応ガイド」の改訂

1. 調査背景・検討概要

- これまで、ウェブサイトの脆弱性対応について資料を制作し啓発を進めてきたが、未だに届出には SQL インジェクションのような深刻度の高い脆弱性も含まれている。これが氷山の一角であると仮定すると、**世の中のウェブサイトには深刻度の高い脆弱性が潜んでいると考えられる。**
- 大規模、中規模の運営者と比較して**小規模の運営者の対応には課題**がある可能性。



修正完了している割合は全体的に高いものの割合は従業員数に比例する傾向にある。

従業員数31名以上は約70%であるが、**30名以下は約55%と修正完了の割合が低い**

図:運営者規模（従業員数）別にみた届出における修正完了済件数の割合
（従業員数が不明であるものは除いて集計、2020年6月15日時点）

■本質的な課題は、小規模の運営者における脆弱性対策を実施するモチベーションが低いことにあると推測されるが、**脅威を理解すれば対応する層、やりくても手段が分からない層には、普及啓発によって改善する可能性**がある。

■**2012年度脆弱性研究会**で、**小規模運営者の実態調査、普及啓発資料の作成を実施**している。
当時との変化を踏まえ、課題解消のため、**再度、調査・検討を実施して、効果的な対策を実施する必要**がある。

2.アンケート調査

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

[成果物]
小規模ウェブサイト運営者の脆弱性対策に関する調査報告書

[調査対象と件数]
対象：2012年度のアンケート調査と同様に小規模ウェブサイト※を運営する組織のウェブサイト担当や情報システム担当
（経年変化を調査するため、可能な限り2012年度のアンケート対象を取り込む。）
有効回答数：300件以上
※小規模とは、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）を目安とするが、有効回答数300件に満たない場合は対象範囲を検討する。

[調査方法]
ウェブアンケート調査または郵送アンケート調査等

[調査項目]
以下の調査項目を全体で30項目程度（選択式、「その他」の記述は必要）
1. ウェブサイトの構築・運用の形態や内容
2. 脆弱性対策への理解
3. 脆弱性対策の現状と課題
4. IPAの普及啓発資料に関する認知度（活用度）
5. 仮説を検証するための設問（仮説を立てて設問を作成）

3.2012年度調査からの継続設問と仮説

■ 下記、赤字は本年度修正する仮説、灰色は本年度削除する設問。

大項目	No.	仮説内容	対応	問No.
ウェブサイトの構築・運用の実態	仮説1	自社社員が少人数（ほぼ1名）で運用者が不明確	予備調査	問9
			本調査	問7
				問19
	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
				問16
	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 →本年度の仮説修正：セキュリティ対策は運用段階での対策を実施している	本調査	問12
				問13
脆弱性対策への理解	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
			本調査	問11
				問14
	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
				問14
脆弱性対策の現状と課題	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)
				問20(8)
				問20(9)
	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
				問20(1)
				問20(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	本調査	問6
				問20(2)
脆弱性対策の現状と課題	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
				問17
				問18
IPAの普及啓発資料に関する認知度	仮説10	無償で利用可能な良いコンテンツがあるならば利用したい	本調査	問21
				問22

4.2012年度調査からの継続設問（予備調査項目）

大項目	番号	質問対象	質問内容	SA／MA
勤務先	問1	全員	あなたの**勤務先の従業員数**を数えてください。	SA
	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。	SA
	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。	SA
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	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。	SA
	問5	自社のウェブサイトに関わっている方※1	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。	MA
	問6		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。	MA
	問7	他社（顧客）のウェブサイトに関わっている方※	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。	MA
	問8		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。	MA
	問9	全員	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。	SA
	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。	MA
	問11		あなたの会社での**担当業務**をお答えください。	SA

※1：問4の回答から判断する。

4.2012年度調査からの継続設問（本調査項目）

大項目	番号	質問対象	質問内容	SA／MA
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	問1	全員	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。	SA
	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。	MA
	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。	SA
	問4	外部サービス等を利用しウェブサイトを運用・管理する方※2	**ウェブサイトの保守・運用**については、主に**どのような作業を外部事業者に委託**していますか。あてはまるものをお答えください。	MA
	問5	全員	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。	SA
	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。あてはまるものを全てお答えください。	MA
ウェブサイトのセキュリティ対策全般の状況	問7	全員	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。	SA
	問8		貴社ではウェブサイトの**セキュリティ対策を外部委託**していますか。	SA
	問9	一部または大半を外部委託している方※3	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。	SA
	問10		委託先から**具体的なセキュリティ対策について報告文書**を取得していますか。	SA

※2：問3の回答から判断する。※3：問7の回答から判断する。

※灰色は、削除する設問。

4.2012年度調査からの継続設問（本調査項目）

大項目	番号	質問対象	質問内容	SA／MA
ウェブサイトの脆弱性に関する取組み	問11	全員	**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。	SA
	問12		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。	MA
	問13		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。	MA
	問14	脆弱性対策はしていない方※4	**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。	MA
	問15	全員	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。	MA
	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。	SA
	問17		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。	SA
	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。	SA
	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。	SA

※4：問12の回答から判断する。

※灰色は、削除する設問。

4.2012年度調査からの継続設問（本調査項目）

大項目	番号	質問対象	質問内容	SA／MA
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	問20	全員	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。	SA
脆弱性対策に関する公的な取組みの認知状況	問21		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。	SA
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	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。 ※選択肢に「安全なウェブサイトの作り方」や脆弱性対策情報ポータルサイト JVN等のコンテンツ10項目	SA
	問23		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。	MA

※灰色は、削除する設問。

5.本年度調査の追加・修正設問と仮説

■ 本年調査の追加(案) を赤字で示す。

No.	仮説内容	対応	問No.	質問内容
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）	本調査	追加1	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**。
追加仮説1	基本的なセキュリティ対策は、10年前と比較しても変化せず、実施している中小企業は少ない	本調査	追加2	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。
追加仮説2	ウェブサイトの役割や重要性が高まっているが、脆弱性対策やセキュリティ対策にかけるコストは変わらない	本調査	追加3	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？
			追加4	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？
			追加5	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？
			追加6	この10年くらいで、貴社の**ウェブサイトの運用(管理や更新作業を含む)に掛かるコスト**がどの様になりましたか？
追加仮説3	クラウド等のサービス利用時に、セキュリティ対策は、サービス提供事業者が対応しているので、自組織の対応が不要と思っている	本調査	追加7	[外部サービス利用と回答した方にお尋ねします] 開発・構築及び運用・管理で利用しているサービスのセキュリティ対策については、**自社の責任範囲とサービス提供者の責任範囲が明確**になっていますか。
追加仮説4	運用時の脆弱性対策として何らかの対応が実施されてはいるが、複数の対策による複合的な対応まではなされていない	本調査	追加8	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。

4.本年度調査の追加・修正設問（本調査項目）

番号	質問対象	質問内容	SA／MA
追加1	全員	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**。 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：　　）	SA
追加2	全員	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、選択肢：実施している、実施したことはない a.ソフトウェアの定期的な更新 b.セキュリティ製品利用 c.パスワードの管理・認証の強化 d.定期的な設定の見直し e.脆弱性（脅威、手口など）の最新情報取得	SA
追加3	全員	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？ 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	SA

4.本年度調査の追加・修正設問（本調査項目）

番号	質問対象	質問内容	SA／MA
追加4	全員	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**がどの様になりましたか？ 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	SA
追加5	全員	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？ 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	SA
追加6	全員	この10年くらいで、貴社における**ウェブサイトの運用(管理や更新作業含む)に掛かるコスト**がどの様になりましたか？ 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	SA

4.本年度調査の追加・修正設問（本調査項目）

番号	質問対象	質問内容	SA／MA
追加7	外部サービス等を利用しウェブサイトを運用・管理する方※5	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。 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	SA
追加8	全員	貴社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、選択肢：頻繁に実施する、たまに実施する、実施したことはない a.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） b.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） c.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） d.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） e.セキュリティ製品の導入や更改 f.セキュリティ診断 g.不正な通信の遮断、通信のフィルタリング h.その他（具体的に：　　）	SA

※5：問1・問3の回答から判断する。

アンケート調査項目に関する参考情報

参考-1. 今回調査で追加した設問と理由
参考-2. 前回調査から削除した設問と理由
参考-3. 前回調査の仮説検証結果

参考-1. 今回調査で追加した設問と理由

問No.	質問内容	理由
追加1	国内のウェブサイトで脆弱性を悪用した**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。	ガイド改訂を検討するにあたり、被害事例の認知度や認知後の対応（行動を実施するか）について確認する
追加2	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。	ガイド改訂を検討するにあたり、基本的な脆弱性対策の実施度合いを確認する
追加3	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？	2012年(頃) と現在の状況変化をアンケート回答内容の変化から分析するだけでなく、直接的にアンケート回答者に確認する
追加4	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**がどの様になりましたか？	
追加5	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？	
追加6	この10年くらいで、貴社の**ウェブサイトの運用(管理や更新作業を含む)に掛かるコスト**がどの様になりましたか？	
追加7	[外部サービス利用と回答した方にお尋ねします] 開発・構築及び運用・管理で利用しているサービスのセキュリティ対策については、**自社の責任範囲とサービス提供者の責任範囲が明確**になっていますか。	2012年以降、クラウド関係のサービスが急速に進展しているため、クラウドを含めたITサプライチェーンにおける責任分界が明確になっているかを確認する
追加8	貴社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。	2012年の設問では、運用時に実施している具体的な脆弱性対策がわからないため、これらを確認する

参考-2. 前回調査から削除した設問と理由

大項目	番号	質問対象	質問内容	SA／MA
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	問4	外部サービス等を利用しウェブサイトを運用・管理する方	**ウェブサイトの保守・運用**については、主に**どのような作業を外部事業者に委託**していますか。あてはまるものをお答えください。 **削除理由** ・問3の設問から外部委託の有無について判断できる。 ・設問内容がセキュリティ以外のウェブサイト運営一般に関する内容であることから、セキュリティ関係の設問を優先するため削除。	SA
ウェブサイトのセキュリティ対策全般の状況	問8	全員	貴社ではウェブサイトの**セキュリティ対策を外部委託**していますか。 **削除理由** ・問7と統合。	SA
	問10	全員	委託先から具体的な**セキュリティ対策**について**報告文書を取得**していますか。 **削除理由** ・2012年度調査では外部委託を実施しているのは、3割程度と少ない。 ・外部委託前提の設問は有効回答数が少なくなるため、外部委託に関する設問は問9のみとし、問10は削除。	SA
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	問23	全員	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。 **削除理由** ・IPAが直接に担当する事業等に関する設問ではないことから、新規に設問を追加するにあたって削除。	SA

参考-3. 前回(2012年度)調査の仮説検証結果

分類	仮説	結果
(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52.7%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」企業は49.3%と多く、「担当者がいる」企業は20.2%、「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」企業は17.3%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）のは関与の状況は、「トップ自らが運用・構築にあたっている」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55.4%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」が判断する企業は34.6%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」企業が全体の56.0%と最も多く、次いで「運用時にのみ対策をしている」企業が22.5%であった。「構築時にのみ対策をしている」企業は皆無（0.5%）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の必要に応じた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」企業も20.9%と多かった。
(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）	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を対象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」（57.5%）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、**脆弱性については知識があり、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。
	(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	

参考-3.前回(2012年度)調査の仮説検証結果

分類	仮説	結果
(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、**脆弱性修正に伴う問題について課題とする意識が高くはない**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」（8.2%）、「おおむね確保できている」（33.0%）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」（19.3%）、「まったく足りていない」（16.9%）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22.6%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)） **従業員数が多い企業においては、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（60.1%）、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ている回答は全体の約7割であった。（本調査 問20(2)）
	(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4.5%、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9.9%あった。これらを合わせると実に15%近くの回答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25～30%ほどが聞いたことがあるとしている。（本調査 問22） 利用してみたいウェブサイトセキュリティ関連の普及・啓発コンテンツについて尋ねたところ、何らかの**コンテンツを利用してみたい**と答えた回答は65.5%であった。