資料１－３

2022年度EC加盟店サイトセキュリティガイドライン検討委員会

一部（非公開＋委員限り）

本事業の概要

2022年９月２日

独立行政法人情報処理推進機構
セキュリティセンター

目次構成

１．本事業の概要

２．ヒアリング調査の進捗状況に関する報告

３．脆弱性診断の進捗状況に関する報告

1．本事業の概要

2．ヒアリング調査の進捗状況に関する報告

3．脆弱性診断の進捗状況に関する報告

本委員会の位置付け

■R3補正事業（中小企業海外展開等支援事業費補助金：ＥＣサイトの脆弱性診断及び対策ガイドライン・モデル契約の提示によるセキュリティ対策の強化）

■ 補正事業の背景

- ECサイトからのクレジットカード番号および個人情報の流出事件が多数（年間約100件)発生し、そのうち中小企業の自社構築サイトが大半を占めている。
- 中小企業の自社構築サイトにおいては、割賦販売法でカード番号非保持化が義務付けられているものの、セキュリティ意識が十分でなく、脆弱性対策が不十分であることがその原因と考えている。

※１　本事業は本状況の改善を目指した、METIサイバーセキュリティ課、商取引監督課の共管事業(個人情報保護委員会とも連携）

■委員会の位置付け：**本事業で作成するセキュリティ対策ガイドラインの内容および効果的な普及・啓発方法に関して有識者からのご助言を頂く**、ことを目的とする。

※２　ガイドラインは自社構築ECサイトからのクレジットカード情報および個人情報漏洩の技術的対策をスコープとします。割賦販売法の義務を履行しているか否か、そして義務の範囲が適当であるかは、今回の事業（委員会）のスコープ外とします。

■連携団体先：クレジット取引セキュリティ対策協議会、JADMA（日本通信販売協会）

本事業の概要

①直近で被害を受けたECサイトへのヒアリング　20社

- 被害の内容・事業への影響、被害時の保守契約の状況、被害後にとった対策、教訓等を把握。

②ECパッケージベンダ、ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング　15社

- 各ベンダのセキュリティ対策状況、保守契約のメニュー等を把握。
- EC-CUBE等パッケージベンダ、EC-CUBEのインテグレーションパートナー等構築事業者、Base、Shopify等ショッピングカートASPベンダが対象。

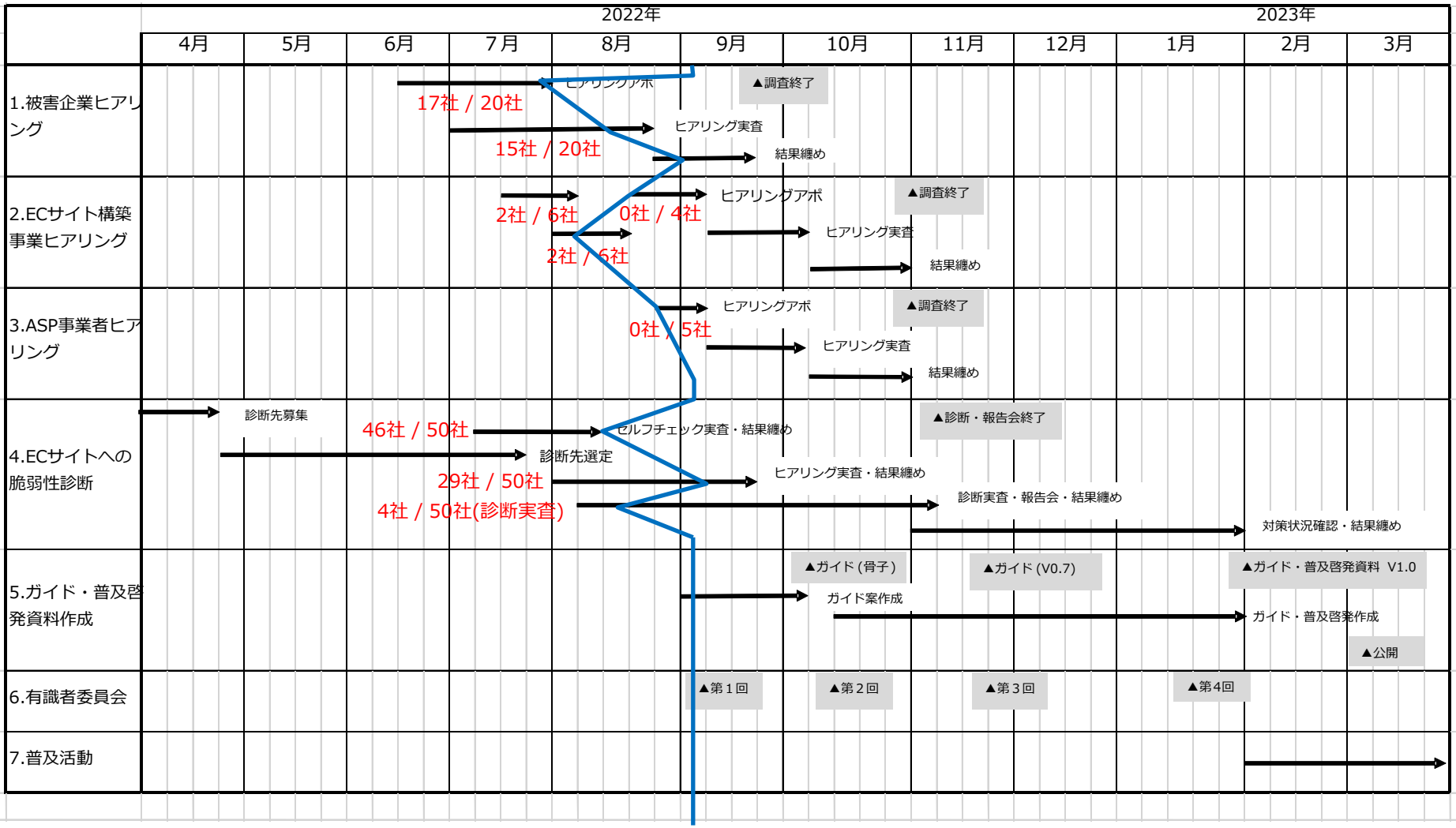
③中小企業の自社構築ECサイト（EC-CUBE等のOSSまたはパッケージを使用したり、スクラッチ開発で構築しているECサイト）に対する脆弱性診断の実施　50サイト

- 対象は数万サイト、公開募集を実施、年商規模、使用パッケージ、業種等がばらける形でMETIと選定。
- 脆弱性診断環境等の事前確認のためのヒアリング、脆弱性診断によりECサイトのセキュリティ対策状況を把握。脆弱性診断の結果と対策助言に関する報告会の開催。脆弱性診断から 3 カ月後を目安にその後の対策状況を確認。

④ECサイト向けセキュリティ対策ガイドライン作成

- 上記①～③の成果をガイドラインとしてまとめる。中小企業経営者向けのチラシを作成。
- 適切な業界チャネル・広告手段を用い成果を配信。

本事業のスケジュール



非公開＋委員限り

①直近で被害を受けたECサイトへのヒアリング

内容は非公開

①直近で被害を受けたECサイトへのヒアリング

調査項目

調査の観点	調査テーマ	調査項目
被害の概要	被害の概要	現在判明している調査結果として、貴社では、いつ頃、何に対して、どのような被害が確認されましたか。
	被害による影響	発生した被害によって、ECサイトを閉鎖しましたか。また、どのような影響が生じましたか、具体的な内容を教えてください。
	被害の発生原因	被害に繋がる一連の問題事象の中で、根本原因は何でしたか。また、最終的に被害に直接的に結び付いた原因は何でしたか。
	被害損失	被害がもたらした損失（機会損失、事故対応費用等）は、金額換算でどれぐらいになりましたか。
被害発生時に必要となった対応	被害が確認されるまでの経緯	被害が確認(特定)されるまでの経緯（被害に繋がる問題事象を認知するまでの時系列でみたプロセスなど）について教えてください。
	被害確認後および被害への長期的な対応局面の対応	被害が確認(特定)された直後、および被害への長期的な対応局面において、貴社はどのような対応を行いましたか。
被害発生時点におけるセキュリティ対策の実装状況	被害発生時点に実装していたセキュリティ対策の内容	被害発生時点の貴社が運営するECサイトについて、当時の開発・構築体制や、運用・保守体制は、どのようになっていましたか。ベンダーがサイトの開発・構築に携わる場合に、ベンダーとの契約の中で、どのようなセキュリティ対応が盛り込まれていましたか。また、サイトの運用・保守に関して、ベンダーとの契約は結んでいましたか。サイトの運用・保守に係る契約の中で、どのようなセキュリティ対応が盛り込まれていましたか。

①直近で被害を受けたECサイトへのヒアリング

調査項目（前ページからの続き）

調査の観点	調査テーマ	調査項目
被害発生後におけるセキュリティ対策の取組状況	被害確認後に実装したセキュリティ対策の内容	被害が確認(特定)された後、被害の発生原因（根本原因、被害に結び付いた直接的な原因）を取り除くため、新たなセキュリティ対策を実装しましたか。当該対策が必要となった理由や追加対策の考え方を含めて教えてください。逆に、被害の発生原因となったものに対して、新たなセキュリティ対策を実装しなかった場合(残存リスクを許容している場合)があれば、その理由や対策の考え方を含めて教えてください。
		被害が確認(特定)された後、ECサイトのセキュリティを強化するため、新たなセキュリティ対策を実装しましたか。当該対策が必要となった理由や追加対策の考え方を含めて教えてください。
		ASPサービスへの移行について実施しましたか。(実施している場合)ASPサービスへの移行について判断した理由について教えてください。
	被害から得られた示唆・教訓	被害を振り返って、被害を受ける前に、これだけは実施しておけばよかったと後悔に繋がっている必要対策や向き合うべき対応はありましたか。
		これだけは実施しておけばよかったと後悔に繋がっている必要対策について、必要である理由、被害を受ける前に実施しなかった理由は何でしたか。

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング（予定）

ECパッケージベンダについては、市場シェアの高い企業を中心に選定し、以下の事業者を調査対象とした。

サービス名	事業者名	主な選定理由
EC-CUBE	株式会社イルグルム	• EC構築オープンソースとして国内シェア1位[*1] • カートシステムとして、利用数が月商1000万円未満で2位、1000万円以上で1位[*2] ヒアリング済み
Welcart	コルネ株式会社	• ECプラグインとして国内シェア1位 • 25,000以上のサイトで利用
shop serve	株式会社Eストアー	• Commerce21を買収 • EC構築業売上高ベース国内シェア1位[*3]

[*1]IPA：第3回オープンソースソフトウェア活用ビジネス実態調査（2009）
[*2]ECマーケティング株式会社：ネットショップ動向調査（2020） https://www.ecmarketing.co.jp/contents/archives/1045
[*3]富士通キメラ総研：ソフトウェアビジネス新市場2019年版（2019）

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング（予定）

ECサイト構築ベンダについては、EC-CUBEのプラチナランクのインテグレートパートナーからサイト構築の事例数の多い事業者や、セキュリティ重視の姿勢がみられる事業者を中心に選定し、以下の事業者を調査対象とした。

事業者名	主な選定理由
株式会社Refine	• ECサイトの構築実績数が全パートナーで最多となっている（サイト構築事例数126、プラグイン事例数31）
株式会社ジョーレン	• ISMS認証を取得 • Webアプリケーションのセキュリティ診断サービスを提供 ヒアリング済み
株式会社アイディーエス	• 創業24年の老舗、AWSの専門部隊を保有 • 自社において、セキュリティ要件を作成し公表

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング（予定）

その他のECサイト構築ベンダについては、EC-CUBE以外のパッケージに関するインテグレートパートナーを中心に選定し、以下の事業者を調査対象とした。

事業者名	主な選定理由
株式会社ガジェログ	• Welcart、EC-CUBEのインテグレートパートナー • 大手モール、Shopifyのサイト構築に対応
ソーバル株式会社	• Welcart、EC-CUBEのインテグレートパートナー • セキュリティ対策や運用・保守サポートのメニューを提供 • STORES、Shopifyでの構築にも対応
日本システム開発株式会社	• Commerce21、EC-CUBE（プレランク）のインテグレートパートナー • 運用・保守の代行対応、小規模～大規模（100億円超）に対応 • ISO/IEC 27001取得
コロニーインタラクティブ株式会社（カゴラボ）	• EC-CUBEのインテグレートパートナー • ソーシャルログイン対応、Shopifyのサイト構築に対応 • クラウドサーバ環境がメイン（カスタムプランあり）

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング（予定）

ショッピングカートASPベンダについては、導入事例数の多い事業者や、セキュリティ重視の姿勢がみられる事業者等多様な観点から選定し、以下の事業者を調査対象とした。

サービス名	事業者名	主な選定理由
ecforce	株式会社SUPER STUDIO	• D2C特化の機能が充実 • 独自のセキュリティ対策（暗号化、脆弱性診断、ログイン制限等）
COLOR ME	GMOペパボ株式会社	• 導入事例数が国内最多 • スマホ用各種管理アプリを提供、デジタルコンテンツ販売が可能
futureshop	株式会社フューチャーショップ	• デザインの自由度や外部連携が充実、バージョンアップが頻繁 • セキュリティ対策ガイドを策定
BASE	BASE株式会社	• Wordpressと連携可能（コード埋め込み、API、プラグイン） • 初期費用0円、手数料が低い
MakeShop	GMOメイクショップ株式会社	• 2021年流通額1位 • 越境EC、多様な決済手段、セキュリティ対策

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング

ECパッケージベンダに対するヒアリング調査項目

調査の観点	調査テーマ	調査項目
セキュリティ対策の概要	セキュリティ対策の概要	貴社では、自社のパッケージにおいて、どのようなセキュリティ対策を実施していますか。
	パッケージの脆弱性診断について	貴社では、自社のパッケージにおいて脆弱性が発見された際、どのように対応するか指針等が決まっていますか。また、利用者への通知等はどのように行っていますか。
		貴社では、自社のパッケージにおける脆弱性情報をどのように収集していますか。
	セキュリティ対策の体制	貴社のパッケージに関するセキュリティ対策は、どのような体制で推進していますか。
		貴社のパッケージに関するセキュリティ対策は、どの程度の頻度で更新されていますか。
	セキュリティ対策の注力項目	貴社のパッケージに関するセキュリティ対策のうち、最も注力している対策はどれですか。
ECサイト運営者のセキュリティ対策の利用状況	利用率	貴社のパッケージを利用するECサイト運営者のおよそ何割が、貴社が提供するセキュリティ対策を利用していますか。
	利用内容	貴社が提供するセキュリティ対策のうち、利用頻度が高いものはどれですか。
	利用が進んでいる企業	貴社のパッケージを利用するECサイト運営者において、貴社が提供するセキュリティ対策を利用する企業は、どのような特徴がありますか。また、その理由は何とお考えですか。
	利用が進んでいない企業	貴社のパッケージを利用するECサイト運営者において、貴社が提供するセキュリティ対策を利用しない企業は、どのような特徴がありますか。また、その理由は何とお考えですか。
	対策案	貴社のパッケージを利用するECサイト運営者において、貴社が提供するセキュリティ対策を利用しない企業は、自社独自にどのような対策を行う必要があるとお考えですか。
ECサイト運営者のセキュリティ対策の内容	契約内容	貴社のパッケージを利用するECサイト運営者は、貴社が提供するセキュリティ対策の利用に際して、セキュリティ運用・保守がどのレベルで実装する取り決め・規定となっていますか。

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング

ECパッケージベンダに対するヒアリング調査項目（前ページからの続き）

調査の観点	調査テーマ	調査項目
ECサイト運営者のセキュリティ対策の内容	インテグレートパートナー	貴社は、貴社のパッケージをECサイト運営者向けに導入する事業者に対して、セキュリティ対策のサポートを実施していますか。
		貴社のパッケージをECサイト運営者向けに導入する事業者は、一般的にECサイト運営者との間で、運用・保守契約に関する責任分界点はどう考えていますか。
	費用	貴社のパッケージを利用するECサイト運営者は、一般的にセキュリティ費用をどの程度負担していますか。
脆弱性診断	提案状況	貴社のパッケージを利用するECサイト運営者に対して、脆弱性診断の提案を行っていますか。
	脆弱性診断を利用する企業	脆弱性診断を行っている場合、利用が多い企業は体制・運用等の観点でどのような特徴のある企業ですか。また、利用が多い理由を何とお考えですか。
	脆弱性診断を利用しない企業	脆弱性診断を行っている場合、脆弱性診断の利用が少ない企業は、体制・運用等の観点でどのような特徴のある企業ですか。また、利用が少ない理由を何とお考えですか。
	提案を行う上での制約状況	貴社のパッケージを利用するECサイト運営者に対して、脆弱性診断の提案を行うに際して、何が制約要因となっていますか。
セキュリティ対策にかけるコスト	算出方法・内訳	セキュリティ対策に係るコストの費用項目や、コストの算出方法について教えてください。
その他	業界団体等に対する要望等	今後、セキュリティ対策の充実強化に向けて、どのような取組を実施すべきか等、業界団体等に対して、何か要望したい事項がありますか。
（EC-Cube様向け）	インテグレートパートナーのランキングの算出基準	プラチナ、ゴールド、シルバー、ブロンズのランキングは、それぞれどのような基準を満たすことが求められますか。またそのような基準には、セキュリティ確保の観点が含まれていますか。

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング

ECサイト構築ベンダに対するヒアリング調査項目

調査の観点	調査テーマ	調査項目
セキュリティ対策の概要	セキュリティ対策の概要	貴社では、EC Cubeの構築支援サービスにおいて、どのようなセキュリティ対策を実施していますか。
	セキュリティ対策の体制	貴社のEC Cubeの構築支援サービスにおいて、セキュリティ対策は、どのような体制で推進していますか。
		貴社のEC Cubeの構築支援サービスにおいて、セキュリティ対策は、どの程度の頻度で更新されていますか。
	セキュリティ対策の利用状況	貴社のEC Cubeの構築支援サービスの中で提供しているセキュリティ対策のうち、最も注力している対策はどれですか。
ECサイト運営者の運用・保守契約の締結状況	運用・保守契約	貴社は、EC構築支援サービスの中で、運用・保守契約を提供していますか。
	契約率	貴社がEC構築を行うECサイト運営者のおよそ何割が、運用・保守契約を締結していますか。
	契約率が高い企業	貴社がEC構築を行うECサイト運営者において、運用・保守契約の契約率が高い企業は、どのような特徴がありますか。また、その理由は何とお考えですか。
	契約率が低い企業	貴社がEC構築を行うECサイト運営者において、運用・保守契約の契約率が低い企業は、どのような特徴がありますか。また、その理由何とお考えですか。
	制約要因	ECサイト運営者に対して、運用・保守契約の提案を行うに際して、何が制約要因となっていますか。
	対策案	貴社がEC構築を行っており、運用・保守契約を締結していないEC サイト運営者においては、自社独自にどのような対策を行う必要があるとお考えですか。
運用・保守契約の内容	契約内容	貴社がEC構築を行うECサイト運営者は、一般的に運用・保守契約の内容の中で、セキュリティ運用・保守がどのレベルで実装されている取り決め・規定となっていますか。
		運用・保守契約の内容の中で、貴社とECサイト運営者との対策分担はどのようになっていますか。
	費用	一般的に運用・保守契約の締結に係るECサイト運営者の費用負担は、どの程度ですか。

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング

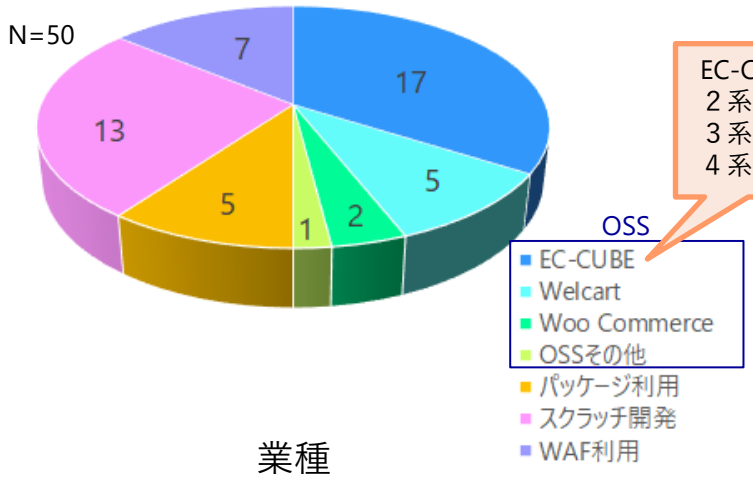
ECサイト構築ベンダに対するヒアリング調査項目（前ページからの続き）

調査の観点	調査テーマ	調査項目
運用・保守契約の内容	事例	運用・保守契約を結んでいるECサイト運営者との間で、実際に対応が必要となったセキュリティインシデントはありましたか。ある場合、具体的にどのような内容でしたか。
		運用・保守契約を結んでいるECサイト運営者との間で、契約終了後に再契約となった事例はありますか。その理由は何とお考えですか
契約書上での記載状況	セキュリティ関連の実施項目の記載状況	貴社がEC構築を行うECサイト運営者との間で、運用・保守契約の中で謳われている、貴社が実施可能なセキュリティ対応の実施項目は何ですか。
		貴社がEC構築を行うECサイト運営者との間で、貴社・ECサイト運営者・およびEC Cubeとの間のセキュリティインシデントにおける責任分界点はどのように考えていますか。
	事例	貴社が提供するセキュリティ対策の実施項目として、ニーズがあるのはどのようなものですか。
脆弱性診断	提案状況	貴社は、貴社がEC構築を行うECサイト運営者に対して、脆弱性診断の提案を行っていますか。
	脆弱性診断を利用する企業	脆弱性診断の利用が多い企業は体制・運用等の観点でどのような特徴のある企業ですか。また、利用が多い理由を何とお考えですか。
	脆弱性診断を利用しない企業	脆弱性診断の利用が多い企業は体制・運用等の観点でどのような特徴のある企業ですか。また、利用が少ない理由を何とお考えですか。
	提案を行う上での制約状況	脆弱性診断の提案を行うに際して、何が制約要因となっていますか。
その他のセキュリティサービス	その他のセキュリティサービスの提案状況	脆弱性診断の提案以外に、セキュリティサービスの提案を行っていますか。セキュリティサービスの具体的な内容について教えてください。
セキュリティの運用・保守コスト	算出方法・内訳	セキュリティの運用・保守に係るコストの費用項目や、コストの算出方法について教えてください。
その他	業界団体等に対する要望等	今後、セキュリティ対策の充実強化に向けて、どのような取組を実施すべきか等、業界団体等に対して、何か要望したい事項がありますか。

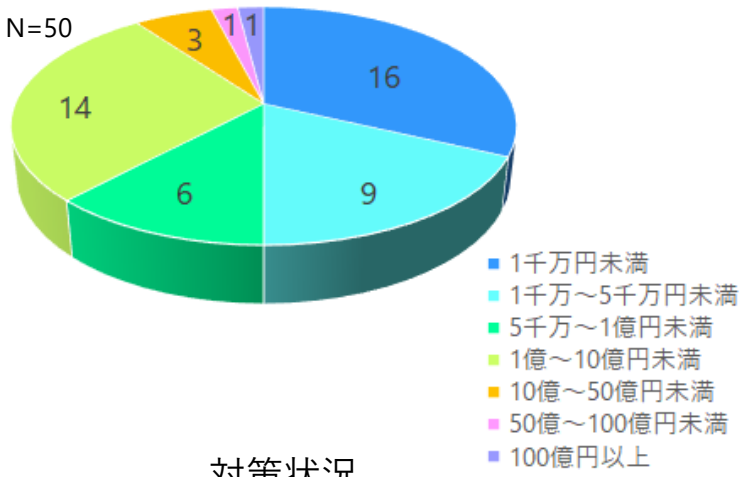
③中小企業の自社構築ECサイトに対する脆弱性診断の実施

・対象：中小企業が運営する自社構築のECサイト（モール、カートASPのECサイトは除く）
・IPAウェブサイトで募集（3/8～4/20）、152サイトが応募
・応募のあったECサイト運営事業者の中から、サイト構築手法/利用OSS、業種、年商、対策状況を踏まえ、バランスを考慮しつつ、診断対象５０サイトを選定

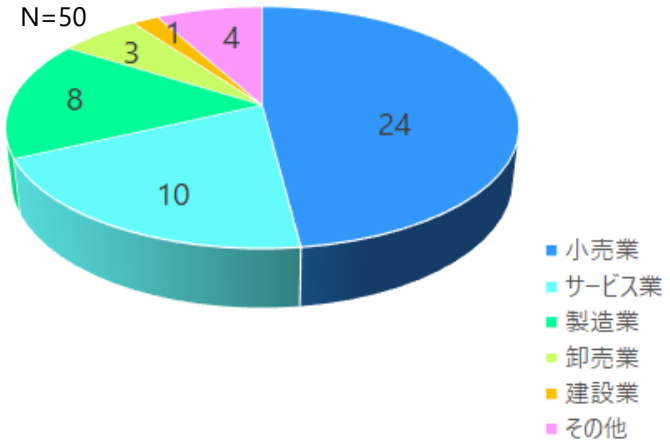
サイト構築手法/利用OSS



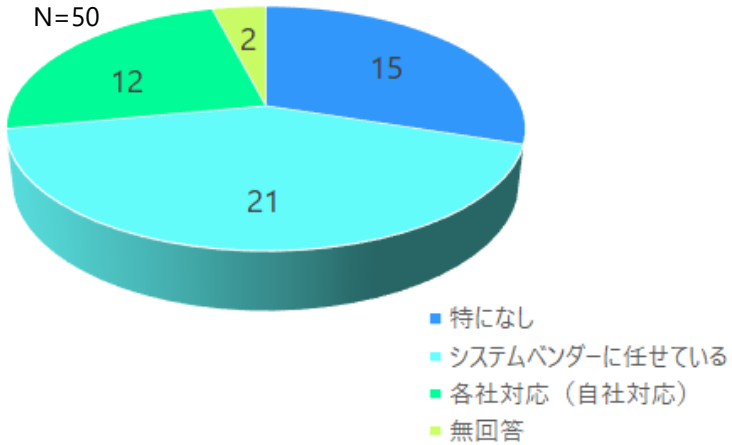
年商



業種



対策状況



非公開＋委員限り

③中小企業の自社構築ECサイトに対する脆弱性診断の実施

内容は非公開

④ECサイト向けセキュリティ対策ガイドライン作成

ECサイト向けセキュリティ対策ガイドラインの構成イメージを以下に示す。

- 第一部　ECサイトにおけるセキュリティ対策
  - ①　はじめに
  - ②　ECサイトが狙われている（ECサイト攻撃からの被害事例、調査結果を踏まえて）
  - ③　なにが問題なのか（ECサイトの脆弱な点、調査結果を踏まえて）
  - ④　攻撃に対しどのように向き合うべきか（対策に対する指針）
  - ⑤　対策をしないと何が起きるのか？（サイトおよび事業停止、お客様への迷惑）
- 第二部　ECサイト構築の各フェーズにおける対策
  - ①　具体的な対策
    - a.　組織的な対策
    - b.　サイト計画時における対策
    - c.　サイト構築時における対策
    - d.　サイト公開時における対策
    - e.　サイト運用時における対策

      ※自社によるECサイト構築と、ショッピングASPカートによるECサイト構築の両方式におけるのメリット・デメリットを定量的に記載
  - ②　ECサイト開発時・運用時における外部発注契約上の注意事項
    - 契約に係る問題点、契約のあり方、注意事項
  - ③　その他
    - 実際に被害にあった際の対応、対策
    - 現在の自組織のセキュリティ状況確認のチェックリスト
- 参考資料

1．本事業の概要

2．ヒアリング調査の進捗状況に関する報告

3．脆弱性診断の進捗状況に関する報告

非公開＋委員限り

①直近で被害を受けたECサイトへのヒアリング

内容は非公開

非公開＋委員限り

②ECパッケージベンダ、 ECサイト構築ベンダ、ショッピングカートASPベンダへのセキュリティ対策状況ヒアリング

内容は非公開

1．本事業の概要

2．ヒアリング調査の進捗状況に関する報告

3．脆弱性診断の進捗状況に関する報告

③中小企業の自社構築ECサイトに対する脆弱性診断の実施

脆弱性診断については、以下に示す 5 つのステップに沿って、実施中。ステップ 4 までを10月中までに完了予定。

【進捗状況】9/2時点

Step1 セルフチェック調査

Step 3 の脆弱性診断に必要な情報として、セキュリティ対策状況、脆弱性診断環境をチェックリストにより把握

Step2 ヒアリング調査

Step 1 のセルフチェック調査により把握した内容について、ヒアリング調査により詳細を確認

Step3 脆弱性診断

本番環境に対するリモートでの脆弱性診断（ネットワーク診断、ウェブアプリケーション診断）を実施

50サイト中、**50サイト**

↓

50サイト中、**29サイト**

↓

50サイト中、**4サイト完了**

Step4 脆弱性診断結果の報告

Step 3 の脆弱性診断の結果について、報告会を開催し、併せて推奨される対策の助言を実施

Step5 フォローアップ調査

Step 4 の脆弱性診断結果の報告を踏まえて、概ね 3 か月後に診断対象企業において新たに対策された内容をメールにて確認