EC サイトへの不正アクセスに関する実態調査

令和4年3月 16 日

個人情報保護委員会

（はじめに）

近年、EC サイト[1]を狙った不正アクセスが多発しており、個人情報保護委員会にも EC サイトへの不正アクセスによる個人データの漏えい等事案が多く報告されている。EC サイトは、クレジットカード情報を含む個人データを盗むことを目的として攻撃の対象になりやすい傾向にあり、こうした EC サイトにおける個人データの漏えい等事案が発生すると、財産的な被害が発生し被害者数も大きくなりやすく、さらには事業者に対する信用の低下にもつながりかねないなど、深刻な被害に陥りやすい。

当委員会では、こうした EC サイトへの不正アクセス対策に資するよう、事業者に対する注意喚起の資料（「WARNING～ウェブサイトを運営している事業者の皆様への注意喚起～」）を公表し、ウェブサイト運営事業者がセキュリティ対策を行う上で注意すべき事項や、発生事例から学ぶセキュリティ対策について示している。

今般、当委員会では、個人データの漏えい等報告を提出した EC サイト運営事業者に対してアンケート調査を実施し、不正アクセス被害に関して、①個人データの漏えい等事案が発生した原因、②事案発生を受けて検討された再発防止策、③漏えい等事案の発生により生じた損失について、調査結果を取りまとめた。

（調査の概要）

（1）調査時期

令和3年8月

（2）調査方法

平成 30 年4月から令和3年3月までに当委員会に個人データの漏えい等報告を提出した EC サイト運営事業者のうち本調査への協力が得られた事業者に調査票を送付した。

（3）回答事業者数

71 事業者

（4）回答事業者の属する業種

卸売業・小売業	製造業	情報通信業	宿泊業・飲食サービス業	生活関連サービス業・娯楽業	その他
62% （44 社）	20% （14 社）	6% （4社）	4% （3社）	3% （2社）	6% （4社）

（5）従業者数

5名未満	5名以上	50 名以上	100 名以上	500 名以上
3% （2社）	38% （27 社）	27% （19 社）	23% （16 社）	10% （7社）

（6）回答部署

管理部門	営業部門	システム部門	その他
28% （20 社）	14% （10 社）	25% （18 社）	32% （23 社）

[1] EC サイトとは、インターネット上で商品を販売するウェブサイト、いわゆるショッピングサイトのこと。

1. 漏えい等の発生原因

- 不正アクセスを受けた EC サイトの運営事業者の多くが、EC サイトの開発・構築、運用・保守を外部の事業者に委託していた。
- 外部委託している事業者において、自社と委託先との間でセキュリティ対策に関する責任範囲を理解しておらず、認識合わせ・合意をしていないとする事業者が多くみられた。セキュリティ対策に漏れが生じないようにするため、委託先との間で、セキュリティ対策の具体的な方法や責任範囲を明確にしておくことが肝要である。
- 不正アクセスの発生理由についての自社の認識として、脆弱性についての理解不足、技術的ノウハウの不足など、情報セキュリティに関する知識面での不足を挙げる事業者が多くみられ、委託先任せの姿勢を挙げる事業者も過半数となっているほか、予算・人的リソースの不足を挙げる事業者も半数近くに及んでいる。

(1) 不正アクセスを受けた EC サイトの開発・構築方法

- 不正アクセスを受けた EC サイトの開発・構築方法として、外部委託により構築（オープンソースの EC サイト構築用プログラムなどでの構築を委託した場合を含む。）していた事業者が最も多い（77%）。
- このほか、自社開発をしていた事業者も2割程度であり、そのうち、オープンソースの EC サイト構築用プログラムなどを利用して構築していた事業者（14%）のほか、独自でアプリケーションを開発していた事業者（6%）もみられた。
- EC 構築向けクラウド型サービスの利用による構築は僅少（3%）であり、ショッピングモール型のサービスを利用していた事業者は、今般の調査対象先に存在しなかった。

自社開発（独自でアプリケーションを開発）	自社開発（オープンソースの EC サイト構築用プログラムを利用して構築）	外部委託による構築（オープンソースの EC サイト構築用プログラムなどでの構築を委託した場合を含む）	EC 構築向けクラウド型サービスの利用による構築	ショッピングモール型のサービス利用
6% （4社）	14% （10 社）	77% （55 社）	3% （2社）	0% （0社）

(2) 不正アクセスの直接的な原因

・ 不正アクセスの直接的な原因として、SQL インジェクション脆弱性[2] (31%)、決済画面の改ざんを引き起こす脆弱性 (37%) といった、EC サイト脆弱性に対する不正アクセスが多くを占めている。

・ このほか、ヒューマンエラーによる EC サイトの管理者画面へのアクセス制限不備が 15%となっている。

SQL インジェクション脆弱性	決済画面の改ざんを引き起こす脆弱性	EC サイトの管理者画面へのアクセス制限不備	その他	分からない
31% (22 社)	37% (26 社)	15% (11 社)	13% (9社)	4% (3社)

(3) 不正アクセスの発生理由についての自社の認識

・ 不正アクセスの発生理由についての自社の認識として、脆弱性についての理解不足 (66%)、技術的ノウハウの不足 (59%) など、情報セキュリティに関する知識面での不足を挙げる事業者が多くみられた。

・ このほか、委託先任せの姿勢を挙げる事業者も過半数 (59%) となっているほか、予算・人的リソースの不足を挙げる事業者も半数近く (44%) に及んでいる。

		該当する	該当しない	無回答
①	脆弱性についての理解不足	66% (47 社)	32% (23 社)	1社
②	委託先任せの姿勢	59% (42 社)	39% (28 社)	1社
③	技術的ノウハウの不足	59% (42 社)	39% (28 社)	1社
④	リスク意識の欠如	44% (31 社)	55% (39 社)	1社
⑤	予算・人的リソースの不足	44% (31 社)	55% (39 社)	1社

[2] SQL インジェクション脆弱性とは、利用者からの入力情報を基に組み立てられるデータベースへの命令文 (SQL 文) に対して適切な取扱いをしていないことに起因して、データベースを不正に操作される脆弱性であり、この脆弱性を利用した攻撃のことを SQL インジェクション攻撃と呼ぶ。この攻撃により、ウェブサイト運営者が意図していないデータベースの操作が可能となり、データベースに格納された個人データの漏えい、改ざん等の被害を受ける可能性がある。

(4)【1(1)で「外部委託」、「EC 構築向けクラウド型サービスによる構築」を選択した事業者(調査対象の80%、57 社)に対する質問】

(4-1) EC サイトの開発・構築における自社と委託先の責任範囲についての理解、認識合わせ・合意の有無

・ EC サイトの開発・構築における自社と委託先の責任範囲について、理解しておらず、認識合わせ・合意をしていない事業者が多くみられた(38%)。1(3)の回答でみられた脆弱性についての理解不足や委託先任せの姿勢といった自社の認識とも符合している。

責任範囲を理解し、委託先と合意	責任範囲を理解していたが、委託先と合意していない	責任範囲を理解しておらず、委託先とも合意していない	無回答	本質問の対象外(自社開発、モール利用)
25% (18 社)	13% (9社)	38% (27 社)	4% (3社)	20% (14 社)

(4-2) EC サイトの開発・構築に係る委託先との契約書又は仕様書におけるセキュリティ対策に関する記載の有無

・ EC サイトの開発・構築に係る委託先との契約書又は仕様書におけるセキュリティ対策に関する記載の有無について、契約書等にセキュリティ対策の記載がないとする事業者が多くみられ(39%)、このほか契約書等にセキュリティ対策の記載はあるが具体的ではないとする事業者もみられた(15%)。

・ 契約によっては、委託先はウェブサイト作成やパッケージソフト導入のみを請け負うといった形態も想定され、その場合には別途のセキュリティ対策を確保することが求められる。

契約書等にセキュリティ対策の記載がある	契約書等にセキュリティ対策の記載はあるが具体的ではない	契約書等にセキュリティ対策の記載がない	分からない・無回答	本質問の対象外(自社開発、モール利用)
3% (2社)	15% (11 社)	39% (28 社)	23% (16 社)	20% (14 社)

(4-3) EC サイトの開発・構築に係る委託先からのセキュリティ対策に関する提案の有無及び提案への対応

・ EC サイトの開発・構築に係る委託先からのセキュリティ対策に関する提案の有無及び提案への対応について、提案を受けたことはないとする事業者が多くみられた(42%)。

・ 委託先との間で具体的にどのようなセキュリティ対策の実施を求めるのかについて明確にしておくことが肝要であるが、1(4-2)において言及したとおり、仮にウェブサイトの開発・構築を委託した事業者にセキュリティ対策を委託できない場合には、別途のセキュリティ対策を確保することが求められる。

提案を受けて契約を見直した	提案を受けたが見直しをしなかった	提案を受けたことはない	分からない	無回答	本質問の対象外(自社開発、モール利用)
7% (5社)	8% (6社)	42% (30 社)	15% (11 社)	7% (5社)	20% (14 社)

(5) 不正アクセスを受けた EC サイトの保守・運用の形態

・ 不正アクセスを受けた EC サイトの保守・運用の形態として、開発・構築した外部事業者に保守・運用についても委託していた事業者が最も多い(56%)。

・ このほか、自社により保守・運用していた事業者も2割程度であり(21%)、1(1)で自社開発していた事業者と同水準。

・ 保守・運用は特に行っていないとする事業者も1割程度みられた(11%)。

自社	外部委託(開発・構築した外部事業者に委託)	外部委託(開発・構築した事業者とは別の外部事業者に委託)	保守・運用は特に行っていない
21% (15 社)	56% (40 社)	11% (8社)	11% (8社)

(6)【1(5)で「外部事業者への委託による保守・運用」を選択した事業者(調査対象の 67%、48 社)に対する質問】

(6-1) EC サイトの保守・運用における自社と委託先の責任範囲についての理解、認識合わせ・合意の有無

・ EC サイトの保守・運用における自社と委託先の責任範囲についての理解、認識合わせ・合意の有無について、責任範囲を理解しておらず、委託先とも合意していないとする事業者が多くみられ(34%)、1(4-1)の開発・構築に関して責任範囲を理解せず合意もしていなかったとする事業者と概ね同水準。保守・運用業務においても、委託先との間の責任分界点への理解不足が目立つ。

責任範囲を理解し、委託先と合意	責任範囲を理解していたが、委託先と合意していない	責任範囲を理解しておらず、委託先とも合意していない	無回答	本質問の対象外 (自社で保守・運用、保守・運用を行っていない)
20% (14 社)	10% (7社)	34% (24 社)	4% (3社)	32% (23 社)

(6-2) EC サイトの保守・運用に係る委託先との契約書又は仕様書におけるセキュリティ対策に関する記載の有無

・ EC サイトの保守・運用に係る委託先との契約書又は仕様書におけるセキュリティ対策に関する記載の有無について、契約書等にセキュリティ対策の記載がないとする事業者が多くみられ(30%)、1(4-2)の契約書等にセキュリティ対策の記載がないとする事業者(39%)と概ね同じ水準。セキュリティ対策については、開発・構築段階のみならず、保守・運用段階においても、明確に委託内容を検討することが肝要である。

契約書等にセキュリティ対策の記載がある	契約書等にセキュリティ対策の記載はあるが具体的ではない	契約書等にセキュリティ対策の記載がない	分からない・無回答	本質問の対象外（自社で保守・運用、保守・運用を行っていない）
3% （2社）	14% （10社）	30% （21社）	21% （15社）	32% （23社）

（6-3）EC サイトの保守・運用に係る委託先からのセキュリティ対策に関する提案の有無及び提案への対応

- EC サイトの保守・運用に係る委託先からのセキュリティ対策に関する提案の有無及び提案への対応について、提案を受けたことはないとする事業者が多くみられた（28%）。
- 保守・運用の段階においても、委託先との間で具体的にどのようなセキュリティ対策の実施を求めるのかについて明確にしておくことが肝要である。

提案を受けて契約を見直した	提案を受けたが見直しをしなかった	提案を受けたことはない	分からない	無回答	本質問の対象外（自社で保守・運用、保守・運用を行っていない）
8% （6社）	6% （4社）	28% （20社）	20% （14社）	6% （4社）	32% （23社）

2. 再発防止策

- 不正アクセスを受けて、EC サイトの開発・構築を、自社開発や外部委託から、クラウド型サービスによる構築やショッピングモール型のサービスの利用に切り替えた事業者が、多くみられる。
- 不正アクセスを受けた後、多くの事業者が、EC サイトのセキュリティ対策として、①セキュリティ製品の導入、②定期的なソフトウェアの更新、③管理者画面へのアクセス制御の強化又は多要素認証、④WAF の設定見直しや EC パッケージのセキュリティ設定の定期見直し、⑤製品脆弱性の最新情報の収集、⑥定期的なセキュリティ診断を実施している。再発防止策として、これらのセキュリティ対策をできるだけ複数、組み合わせた多層防御を行うことが求められる。
- 不正アクセスを受けた後、自社従業者へのセキュリティ教育の強化やセキュリティ責任者の配置など、管理体制の強化を図った事業者が多くみられた。自社の EC サイトに必要なセキュリティ対策について全て委託先任せとするのではなく、委託元としてもセキュリティ対策に関する知識を有する人材を育成・確保していくことが求められる。

(1) 現在(不正アクセスを受けた後)運営する EC サイトの開発・構築方法

- 現在(不正アクセスを受けた後)において運営する EC サイトの開発・構築方法として、自社開発、外部委託が不正アクセスを受ける前 (20%、77%) からそれぞれ大きく減少した (4%、27%)。
- 一方、クラウド型サービスは大幅増 (3%から 48%に)、ショッピングモール型も増加 (0%から7%に)。
- 自社による EC サイト構築・運用は困難であると判断し、セキュリティ対策が付帯している EC 構築向けクラウド型サービスに切り替えたとの回答が多くみられている。もっとも、1 (1) のとおり、EC 構築向けクラウド型サービスを利用している場合でも不正アクセスによる漏えい等事案が発生しているため、委託先に全てを任せるのではなく、委託元として自社にもシステムセキュリティ対策に関するノウハウを有する人材を育成していくことが肝要である。

自社開発 (独自でアプリケーションを開発)	自社開発 (オープンソースの EC サイト構築用プログラムを利用して構築)	外部委託による構築 (オープンソースの EC サイト構築用プログラムなどでの構築を委託した場合を含む)	EC 構築向けクラウド型サービスの利用による構築	ショッピングモール型のサービス利用	現在は EC サイトを運営していない
1% (1社)	3% (2社)	27% (19 社)	48% (34 社)	7% (5社)	14% (10 社)

(2) EC サイトのセキュリティ対策における要員体制の見直しの有無及び内容

(2-1) 要員体制の見直しの有無

- 不正アクセスを受けた後に、半数以上が要員体制の見直しを行っている (56%)。

大幅に見直した	一部見直した	見直しはしていない	無回答・その他
18% (13 社)	38% (27 社)	39% (28 社)	4% (3社)

【2 (2-1) で「大幅に見直した」、「一部見直した」を選択した事業者 (調査対象のうち 56%、40 社) に対する質問】

(2-2) 要員体制の見直しの具体的な内容

- 要員体制の見直しの具体的な内容として、自社従業者へのセキュリティ教育の実施が最も多い (25%)。
- このほか、セキュリティ責任者を配置する等、管理体制を見直した事業者もみられた (11%)。

自社従業者にセキュリティ教育を実施した	セキュリティ担当者を増員した	セキュリティ責任者を配置する等、管理体制を見直した	それ以外	無回答	本質問の対象外 (見直しはしていない、無回答・その他)
25% (18 社)	6% (4社)	11% (8社)	7% (5社)	7% (5社)	44% (31 社)

(3) 現在の EC サイトに対するセキュリティ対策の実施状況

―― 以下2 (3-1) から2 (3-6) までのセキュリティ対策の実施状況について、「実施している」との回答は、何れも、委託先に実施させている場合も含む。

- EC サイトを運営する多くの事業者において、EC サイトのセキュリティ対策として、①セキュリティ製品の導入、②定期的なソフトウェアの更新、③管理者画面へのアクセス制御の強化又は多要素認証、④WAF の設定見直しや EC パッケージのセキュリティ設定の定期見直し、⑤製品脆弱性の最新情報の収集、⑥定期的なセキュリティ診断を実施しているが、一部の事業者では未実施とされており、それぞれの要否について検証することが求められる。

【ショッピングモール型サービスの利用以外の方法で EC サイトを開発・構築した事業者（2（1）で「自社開発」、「外部委託」又は「クラウドサービス」を選択した事業者（調査対象のうち 79%、56 社））に対する質問】

（3-1）定期的なソフトウェア（OS・ミドルウェア・パッケージ等）の更新（セキュリティパッチの適用等）

定期的なソフトウェアの更新を実施している	定期的なソフトウェアの更新を実施していない	無回答	本質問の対象外（ショッピングモール型のサービス、現在は EC サイトを運営していない）
65% （46 社）	6% （4社）	8% （6社）	21% （15 社）

【以下、2（3-6）まで、EC サイトの運営を継続している事業者（2（1）で「自社開発」、「外部委託」、「クラウドサービス」、「ショッピングモール型のサービス」を選択した事業者（調査対象のうち 86%、61 社））に対する質問】

（3-2）WAF（ウェブ・アプリケーション・ファイアウォール）[3]等のセキュリティ製品の導入（利用するクラウドサービスにおいて導入している場合も含む）

セキュリティ製品の導入を実施している	セキュリティ製品の導入を実施していない	無回答	本質問の対象外（現在は EC サイトを運営していない）
56% （40 社）	17% （12 社）	13% （9社）	14% （10 社）

（3-3）管理者画面へのアクセス制御の強化又は多要素認証 [4]の導入等

管理者画面へのアクセス制御の強化・多要素認証の導入等を実施している	管理者画面へのアクセス制御の強化・多要素認証の導入等を実施していない	無回答	本質問の対象外（現在は EC サイトを運営していない）
62% （44 社）	18% （13 社）	6% （4社）	14% （10 社）

[3] WAF（ウェブ・アプリケーション・ファイアウォール）は、ウェブサイトの脆弱性を突く攻撃に対するセキュリティ対策のひとつ。WAF は、ウェブサイトの前面や途中経路のネットワークに配置し、通信電文を解析・検査し、ブラックリスト遮断・ホワイトリスト許可等のルールに従って脆弱性を悪用した攻撃を検出・低減する対策。

[4] 多要素認証は、各種インターネットサービスにおける不正ログイン対策として、複数の要素（記憶、所持、生体情報）を用いた認証方式。

(3-4) WAF の設定見直しや EC パッケージのセキュリティ設定の定期見直し

WAF の設定見直しや EC パッケージのセキュリティ設定の定期見直しを実施している	WAF の設定見直しや EC パッケージのセキュリティ設定の定期見直しを実施していない	無回答	本質問の対象外 (現在は EC サイトを運営していない)
58% (41 社)	18% (13 社)	10% (7社)	14% (10 社)

(3-5) 製品脆弱性 (セキュリティパッチ、新バージョンなど) の最新情報の収集

製品脆弱性の最新情報の収集を実施している	製品脆弱性の最新情報の収集を実施していない	無回答	本質問の対象外 (現在は EC サイトを運営していない)
68% (48 社)	10% (7社)	8% (6社)	14% (10 社)

(3-6) 定期的なセキュリティ診断

定期的なセキュリティ診断を実施している	定期的なセキュリティ診断を実施していない	無回答	本質問の対象外 (現在は EC サイトを運営していない)
44% (31 社)	35% (25 社)	7% (5社)	14% (10 社)

(4) 【2 (1) で「外部委託」を選択した事業者 (調査対象のうち 27%、19 社) に対する質問】

(4-1) EC サイトの開発・構築に係る委託先との契約書又は仕様書におけるセキュリティ対策に関する記載の有無

- 不正アクセスを受けた後でも、外部委託により EC サイトを開発・構築する事業者において、契約書等に具体的なセキュリティ対策の記載がある事業者よりも、契約書等に十分な記載がないとする事業者の方が多い (17%＝6%＋11%)。
- 契約によっては、委託先はウェブサイト作成やパッケージソフト導入のみを請け負うといった形態も想定され、その場合には別途のセキュリティ対策を確保することが求められる。

契約書等にセキュリティ対策の記載がある	契約書等にセキュリティ対策の記載はあるが具体的ではない	契約書等にセキュリティ対策の記載はない	分からない	本質問の対象外 (自社開発、ショッピングモール型のサービス、現在は EC サイトを運営していない)
7% (5社)	6% (4社)	11% (8社)	3% (2社)	73% (52 社)

3. 漏えい等に伴い発生した損失

- 不正アクセスを受けて個人データが漏えいすることにより、原因等の調査や顧客対応等に多額の費用が発生するほか、EC サイトの運営再開までの間の販売機会を逃すことによる損失も生じる。
- こうした損失を回避するためには、セキュリティ対策を日頃から適切に行うことが肝要である。

(1) EC サイトの停止に伴う損失

- 不正アクセスを受けて、約8割の事業者が一旦 EC サイトを停止した。

EC サイトを停止した	EC サイトを停止しなかった
79% (56 社)	21% (15 社)

- EC サイトの停止期間は1週間から2年以上と幅があるが、半年以上1年未満の回答が最も多かった。
- 具体的な損失金額は、EC サイト上の取引規模や停止期間によりばらつきがみられるが、1,000 万円以上の損失が発生したと回答した事業者が4割以上であり、数億円の損失が発生した事業者もみられた。
- 左下の表は、機会損失額(売上)を従業者数別に集計したもので、従業者数が多くなるほど事業者あたりの機会損失額が増加する傾向がみられた。
- 右下の表は、機会損失額(売上)を EC サイトの閉鎖期間(月数)に応じて集計した表で、長期になるほど機会損失による影響が大きい傾向がみられた。

機会損失額（売上）の分布

■従業者数別 （百万円）

5名未満	5名以上	50名以上	100名以上	500名以上
3	1.2	0.3	4.2	5
	3	1	9	50
	3	2	20	120
	5	5	25	340
	5	5	28	
	8	7	40	
	10	17	50	
	10	20	100	
	10	25	100	
	10	30	150	
	10	50	500	
	10	75	1,000	
	10			
	15			
	15			
	15			
	16			
	20			
	70			

■ECサイト閉鎖期間別 （百万円）

3か月未満	3か月以上	6か月以上	9か月以上	1年以上
10	1	1.5	5	0.3
10	5	5	10	3
	8	9	25	3
	10	10	25	4.2
	16	10		5
	75	15		15
	1,000	15		17
		20		20
		20		30
		70		40
		100		50
		150		100
				120
				340
				500

機会損失額（売上）
10百万円以上
100百万円以上

(2) フォレンジック調査等、原因特定や被害範囲特定を行うための調査の実施

- **不正アクセスを受けて、ほぼ全ての事業者が、フォレンジック調査等、原因特定や被害範囲特定を行うための調査を実施している。**
- **調査を外部に委託した場合の費用としては、100 万円～500 万円が多く、特に 200～249 万円が多い。**

外部機関にて調査を行った	自社で調査を行った	調査を行わなかった
96% (68 社)	3% (2社)	1% (1社)

(3) 顧客からの問合せへの対応

- **不正アクセスによる個人データの漏えい等の発生を受けて、全ての事業者が問合せ対応を行っている。**
- **自社での対応と外部委託を併用したという回答や、自社の通常の問合せ窓口を利用したという回答もみられた。**
- **問合せ対応期間は、3か月間又は6か月間と回答した事業者が多い。**

自社の問合せ窓口で対応した	外部にヘルプデスクを設置した	問合せ対応は行わなかった
68% (48 社)	32% (23 社)	0% (0社)

(4) 不正アクセスによるクレジットカード情報の漏えいに伴う損失

- **不正アクセスを受けて、大半の事業者でクレジットカード情報の漏えいが発生した。**

クレジットカード情報の漏えいがあった	クレジットカード情報の漏えいは無かった	無回答
93% (66 社)	6% (4社)	1% (1社)

(5)【3 (4) で「クレジットカード情報の漏えいがあった」を選択した事業者 (93%、66 社) に対する質問】

(5-1) クレジットカード差替えの手数料の負担

- **クレジットカード差替えの手数料について、大半の事業者が負担しており、差替えに伴う費用について、1件当たり約 2,000 円との回答が6割と最も多かった。**

カード差替えの手数料を負担した	カード差替えの手数料を負担しなかった	本質問の対象外 (クレジットカード情報の漏えいは無かった、無回答)
92% (65 社)	1% (1社)	7% (5社)

(5-2) クレジットカードの不正利用

・ 不正アクセスを受けて、多くの事業者においてクレジットカードの不正利用が発生した。

不正利用が発生した	不正利用は発生しなかった	本質問の対象外 (クレジットカード情報の漏えいは無かった、無回答)
77% (55 社)	15% (11 社)	7% (5社)

(5-3) クレジットカードの不正利用の補填

不正利用の補填を行った	不正利用の補填を行わなかった	無回答	本質問の対象外 (クレジットカード情報の漏えいは無かった、無回答)
77% (55 社)	4% (3社)	11% (8社)	7% (5社)

(6) 顧客への見舞金の支払い・見舞品の送付

見舞金の支払いや見舞品の送付を行った	見舞金の支払いや見舞品の送付を行わなかった	無回答
25% (18 社)	72% (51 社)	3% (2社)

(7) その他発生した費用

・ 不正アクセスに伴う損失として、上記のほか、セキュリティの強化に伴う費用負担、弁護士・コンサルティング費用負担等の回答があった。

4．まとめ

今般の調査により、セキュリティに関する知識不足、認識不足、委託先任せの姿勢などが、不正アクセスを受けてしまった主な要因に繋がったものとうかがわれた。また、外部委託をしている事業者の多くが、自社と外部委託先との間のセキュリティ対策の責任範囲を明確にしていなかったことが明らかになった。外部委託をしている場合には、委託先との契約書又は仕様書においてセキュリティ対策の責任範囲や具体的な方法を明確にしておくことが肝要である。また、セキュリティ対策について全て委託先任せとするのではなく、委託元としてもセキュリティ対策に関する知識を有する人材を育成･確保していくことが求められる。

不正アクセスを受けた後、多くの事業者が、EC サイトのセキュリティ対策を実施していることがわかった。一般的に、複数のセキュリティ対策を組み合わせた多層防御を行うことで、再発防止策がより有効になると考えられるため、事業者においては、こうした観点からのセキュリティ対策の拡充についても検討することが望まれる。

不正アクセスを受けて個人データが漏えいすることにより、実際に、原因究明のための調査や顧客対応等に多額の費用が発生するほか、EC サイトの運営再開までの間の販売機会を逃すことによる損失がかなりの規模で生じたことが明らかになった。こうした損失を回避するためには、上述の内容も含め、セキュリティ対策を継続的に実施することが必要である。

本資料が、EC サイト運営事業者及び EC サイト構築を担うシステム開発事業者等の関係者にとって、有益な参考資料になるとともに、セキュリティ対策を見直す契機となることを期待する。

以　上