資料２

中小規模事業者における安全管理措置を推進させるための取組みについて

令和元年７月９日

１．これまでの委員会の取組み

○　中小規模事業者の声⇒個人情報保護のためにどんな取組みをすればよいのか、
「分からない」、「情報が少ない」、「費用が掛かりすぎる」

○　当委員会ウェブサイトに、以下の参考資料を公表

(1) 中小企業向けＱ＆Ａ（抜粋版）（平成30年7月）
「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するＱ＆Ａ」から、基本的な項目を抜粋したもの

(2) 中小企業のための自己点検チェックリスト（平成30年12月）
中小企業の皆様が、自社で個人情報を安全に取扱うためのルールや体制の有無について、自己点検を実施するための資料として作成したもの

(3) 個人データ取扱要領（例）の使い方（平成30年12月）
個人情報の保護に関する法律についてのガイドライン（通則編）の「（別添）講ずべき安全管理措置」における「中小規模事業者」の参考として作成したもの

これまで公表した資料に加え、
更に実務に即した対応策に関する情報を求める声が増加！

２．「安全管理措置実態調査（オンサイトヒアリング）」の結果について

調査の概要

・調査目的及び調査先
個人データの安全管理措置について、当委員会における今後の取組みや他社の参考となる具体的事例（グッドプラクティス）を収集するため、会社規模・業種毎に強固な安全管理措置を実践していると思料される企業に対し、訪問のうえヒアリングを実施

・主なヒアリング項目
組織概要、個人情報の取扱いに関する考え方、取り扱う個人情報の内容、各安全管理措置（規程の整備状況、組織的/人的/物理的/技術的安全管理措置、委託先の管理）の方法、営業店舗やコールセンター等お客様窓口における個人情報の取扱状況

調査の結果（主なグッドプラクティス）

○　多くの事業者が実施していたもの　　◎　一部の事業者でのみ実施されていたもの

個人情報の取扱いに関する考え方
◎「防災」「食中毒」「プライバシー漏えい」を会社の３大リスクとして位置付けている。
個人データの取扱いに係る規律の整備状況
○業務マニュアルに、業務の流れと各業務に応じた個人情報の取扱いにかかる注意事項が併せて規定されている。

組織的安全管理措置

〇個人情報の取得から廃棄までの流れと、各プロセスにおいて想定されるリスクを列挙した「業務フロー全体図」を作成して、リスクを可視化している。
◎経営全般のリスクを数値化したうえで、現状対応できていない残余リスクを算出し、残余リスクの高いものは積極的に経営資源を投入しており、個人情報保護にかかる取組みもこの枠組みの中で行っている。
◎個人情報を含む電子データは、全て「個人情報管理台帳」と共に専用サーバで一元管理している。

人的安全管理措置

◎担当業務毎に個人情報の取扱いに関して注意すべき点が異なるため、研修内容も担当業務毎に変えている。
◎情報の誤廃棄等のミスが発生した際、情報漏えいが業績に及ぼす影響（対応費用、会社の信用回復に必要なコスト等）を具体的に算定したうえで周知し、情報の安全管理の重要性を再意識させている。
◎シュレッダーは１枚ずつ書類を確認しながら行うという誤廃棄防止のための社内ルール徹底のため、廃棄書類の中に「シュレッダー禁止」と書いた紙を忍ばせ、職員が気づくか抜き打ちチェックしている。

物理的安全管理措置

〇不要な顧客情報を洗い出し、廃棄している。
〇社有パソコンでは、許可されたUSBメモリを使用する場合でも、読込みのみに制限している。

技術的安全管理措置

〇人事異動の際に、自動でアクセス権限を変更することに加え、年１回権限の見直しを実施している。
◎二重認証として、カナ入力を求めており、コスト面を配慮したなりすまし防止策を講じている。

委託先管理

〇委託契約締結後も自社で定めるセキュリティ基準を満たすか継続的にチェックを行っている。
◎委託時には「委託先管理チェックシート」に記入することに加え、個人情報の性質や量により、契約前及び契約後も定期的に委託先に立入検査を実施するルールとしている。

３．「中小規模事業者の安全管理措置に関する実態調査（アンケート調査）」の報告結果について（概要）

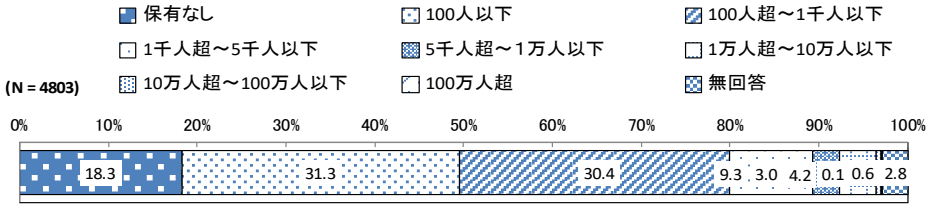
○調査概要

調査目的	事業者の個人データの安全管理措置の実態を把握し、個人情報保護委員会における検討及び今後の執務に役立てるとともに事業者の個人情報保護に対する意識の向上、体制の見直しにつなげること
調査事項	個人情報の保有・利用実態、安全管理措置に関する取組、情報漏えい等、個人情報の取扱いに関する委託等、個人情報を取り巻く課題・要望・変化の状況
調査対象	国内に本社を置く従業員100人以下（※）の事業者３万先（日本標準産業分類を参考に18業種から無作為抽出） （※）「個人情報の保護に関する法律についてのガイドライン（通則編）」は、従業員100人以下の個人情報取扱事業者を原則として「中小規模事業者」としている。
調査主体	株式会社東京商工リサーチ
調査期間	平成31年２月27日から３月18日まで
回 答 率	16.0%
回 答 数	4,803件

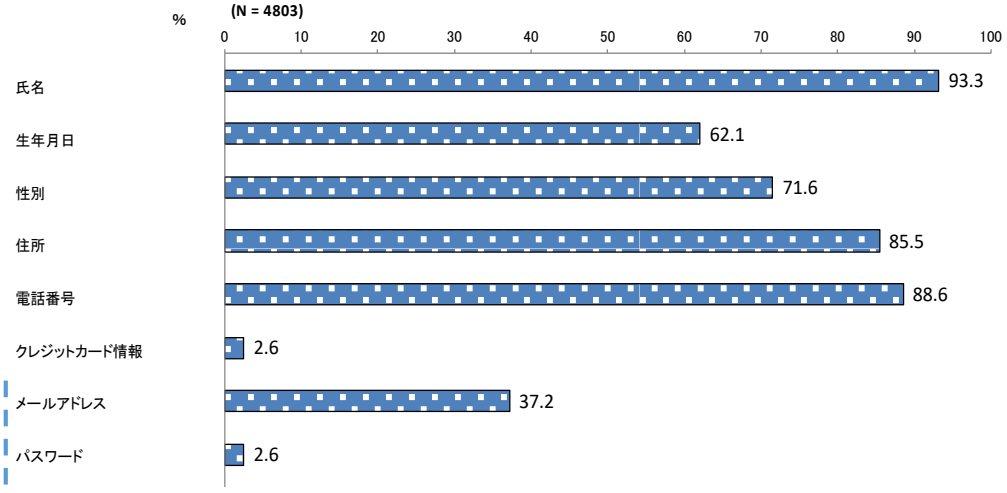
○調査結果（抜粋）

（１）個人情報の保有・利用実態

保有する個人情報の量（顧客情報）

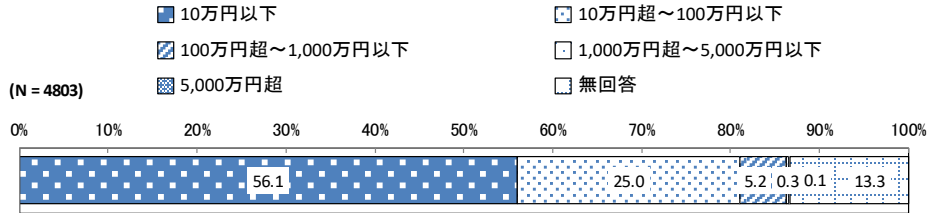


保有する個人情報の内容



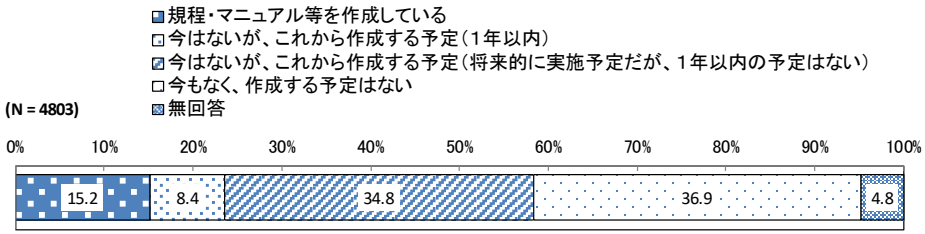
（２）安全管理措置に関する取組

個人情報の安全管理に関する措置に要したコスト

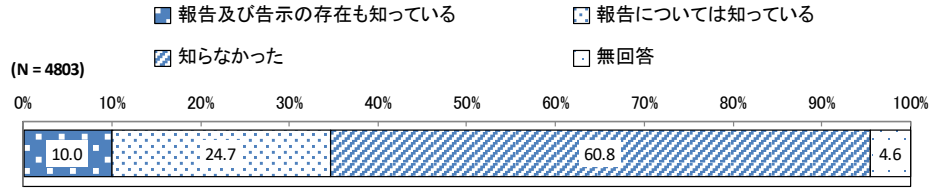


（３）情報漏えい等

個人情報の漏えい等があった場合の対応手順の規程・マニュアルの有無



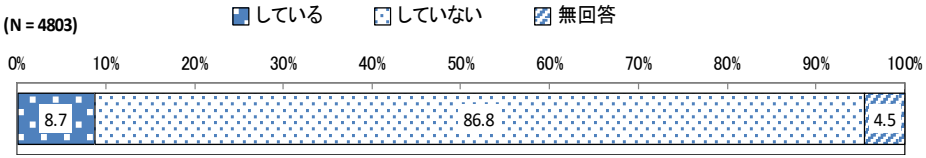
個人情報漏えい等時の個人情報保護委員会等への報告の努め



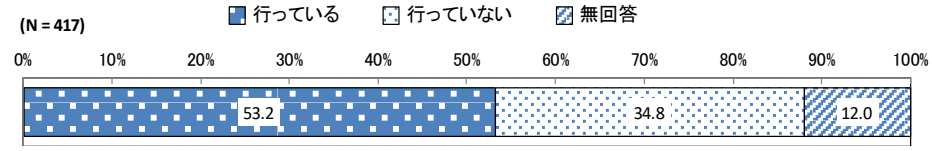
（４）個人情報の取扱いに関する委託等

①外部業者への委託状況

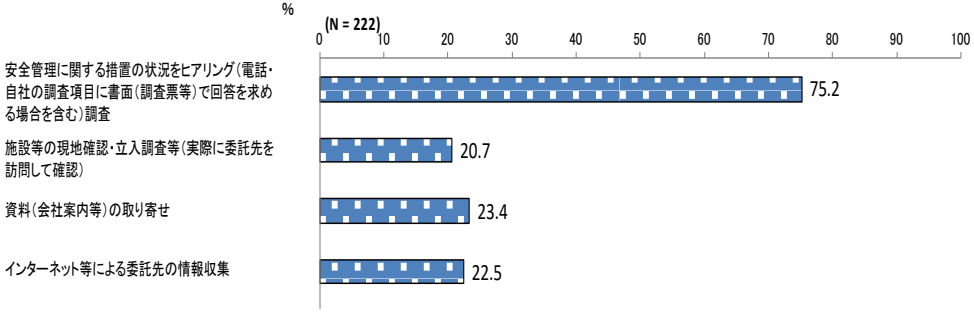
外部業者への委託の有無



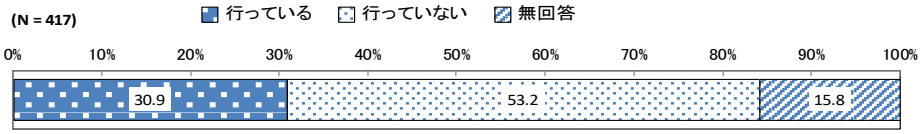
外部委託の実施における、委託先選定に係る事前調査の実施状況



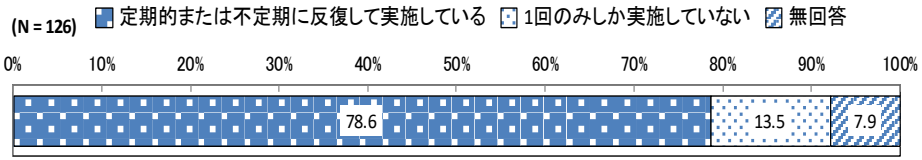
外部委託の実施における、委託先選定に係る調査の方法



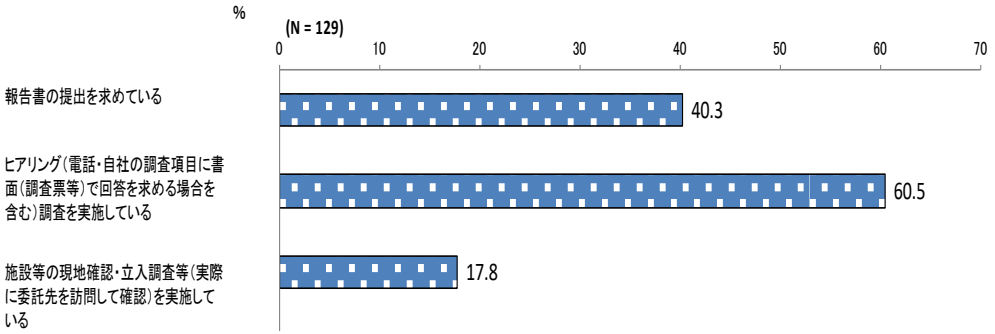
外部委託の実施における、委託先の監督の実施状況



委託先の監督の実施における、委託先監督の頻度

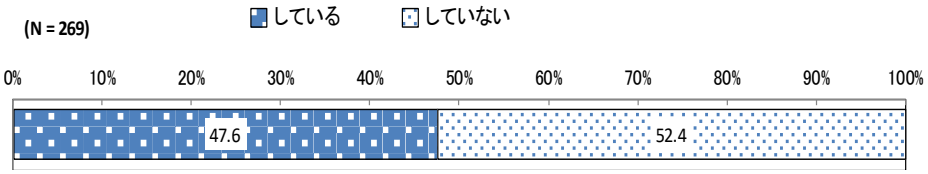


委託先の監督の実施における、委託先監督の方法

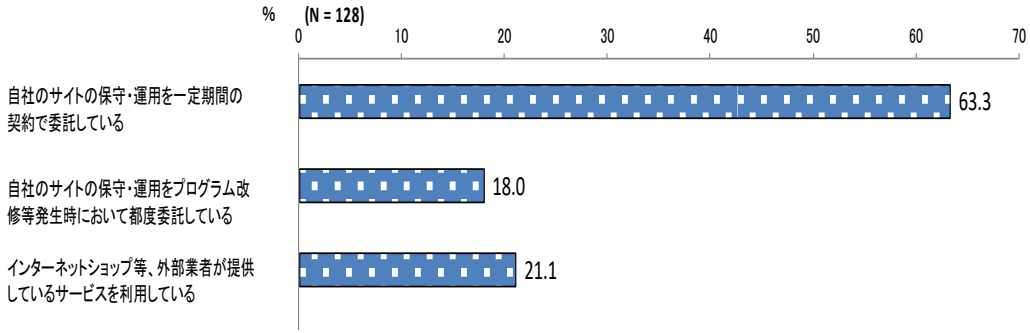


②個人情報を取り扱うウェブサイトの保守・運営業務委託状況

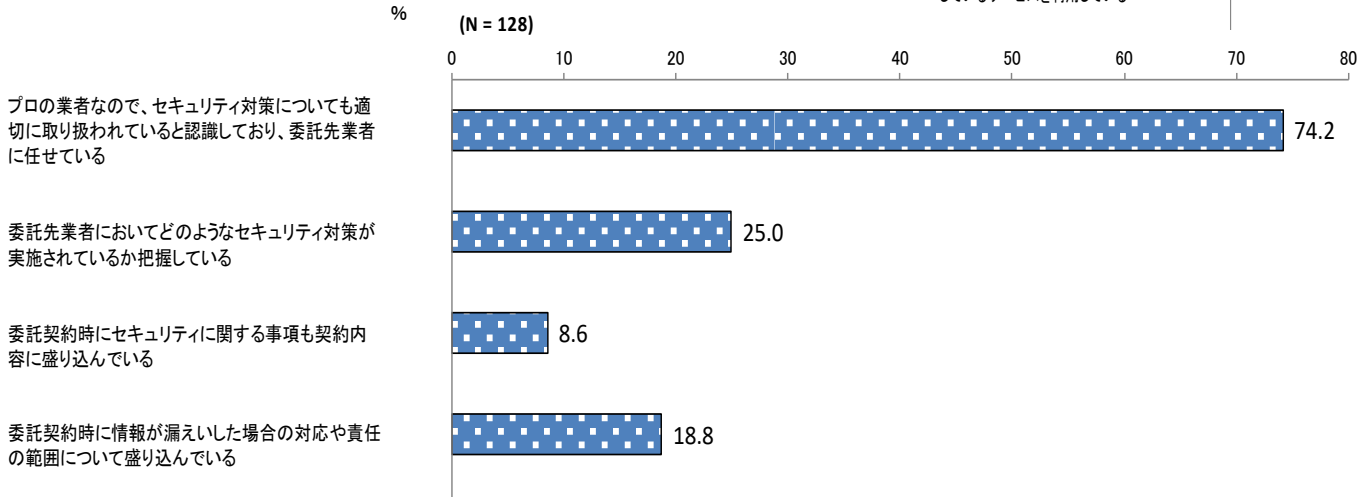
外部委託の実施における、ウェブサイトの保守・運営業務委託の有無



ウェブサイトの保守・運営業務委託における、委託内容

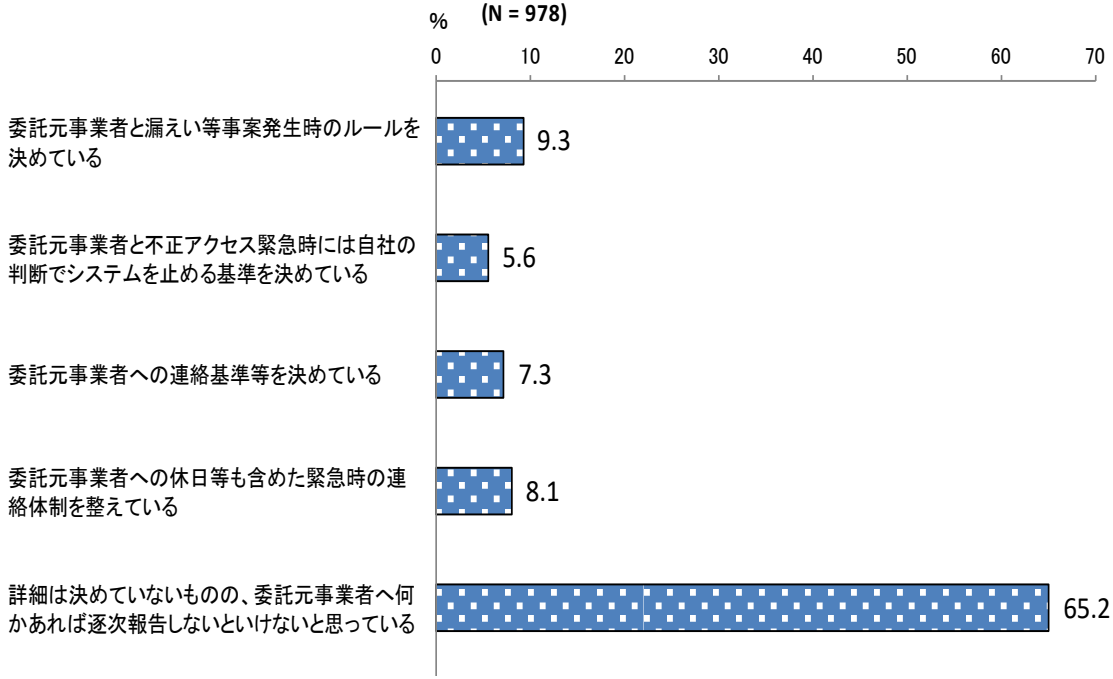


外部委託におけるセキュリティの状況



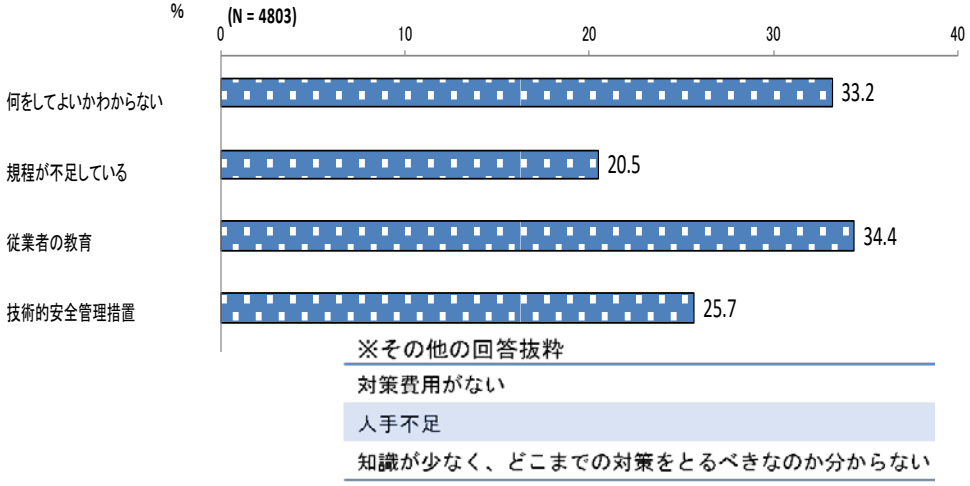
③個人情報を取り扱うウェブサイトの保守・運営業務受託状況

ウェブサイトの保守・運営の受託における、漏えい等発生時の対応

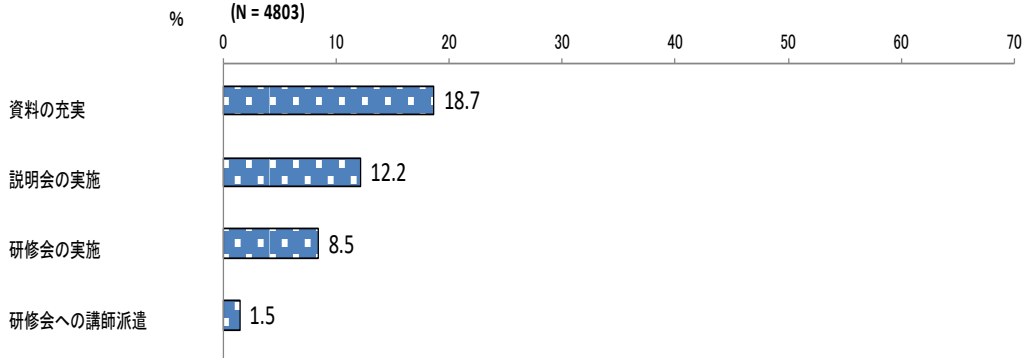


（５）個人情報を取り巻く課題・要望・変化の状況

個人情報の取扱いについて課題と考えていること



個人情報保護委員会へ望む事項



４．個人データの漏えい等事案を受けた対応

漏えい報告に対して注意喚起が必要な事例への対応

- 同様の問題が発生した場合の被害が大きく、他の事業者でも広く発生する可能性がある事案については、委員会ホームページにおいて注意喚起を掲載。
- 特に、ＥＣサイトなどのＷＥＢサイトを運営している事業者に対しては、実際に発生した不正アクセスによる情報漏えい等の事例を踏まえた注意喚起を「ＷＡＲＮＩＮＧ」として委員会ホームページに掲載。

＜掲載事例＞
- 既知の脆弱性対策を怠っていたことによる情報漏えい事案
- ＳＱＬインジェクション攻撃による情報漏えい事案
- リスト型攻撃による情報漏えい事案
- ウェブサイトの機能拡張やバージョンアップに起因して情報漏えいした事案
- 脆弱性診断ツールで脆弱性を検知できず情報漏えいした事案
- 委託先業者のウェブサイトが攻撃され情報漏えいした事案
- 通販サイトを改ざんされてクレジットカード情報が窃取された事案

掲載先ＵＲＬ：　https://www.ppc.go.jp/personalinfo/hiyarihatto/

中小規模事業者において委託契約にセキュリティ対策が含まれていなかった事案があり、同様の問題を注意喚起するために「ＷＡＲＮＩＮＧ」に事例として追加して改版（次頁）

事例８　中小企業において委託契約にセキュリティ対策が含まれていなかった事例

事例

- 情報システムに詳しい社員がいない事業者が、構築・運用保守をシステム事業者に委託してECサイトを立ち上げた。しかし、保守契約における作業範囲にセキュリティ対策は含まれていなかった。
- 稼働から数年経ったある日、クレジットカード決済代行業者より、ECサイトからお客様のクレジットカード情報が漏えいしている可能性があるとの連絡があった。
- フォレンジック調査の結果、システムの脆弱性を突かれて不正アクセスを受けていた可能性が判明した。事業者は保守作業にセキュリティ対策も含まれていると思っていたが、あらためて保守契約書を確認したところそのような記載はなかった。

POINT

- ECサイトの構築・運用保守の委託を契約する際に、適切なセキュリティ対策を必ず盛り込んでおく必要があります。
- 情報システムに詳しい社員がいないからといって、委託先に全てを任せることは望ましくありません。委託元として何を委託し、委託内容が確かに実施されているかなど、適切に確認して管理する必要があります。

対策例

- 運用保守の契約内容に、必要なセキュリティ対策に関する事項が盛り込まれていることを確認しましょう。
- 委託先に全てを任せるのではなく、社内にも情報セキュリティのわかる社員を育成するために、中小企業向け情報セキュリティ対策資料や、企業向けセキュリティ対策セミナーなどを活用し、情報セキュリティに関する知識の習得に努めましょう。

５．実態調査結果等を踏まえた今後の取組み

（１）各種資料の充実

・当委員会ウェブサイトに掲載する**注意喚起等のコンテンツ（個人情報ヒヤリハットコーナー等）をより充実**させる

・既存資料の内容を軸として、**安全管理措置に関するより具体的な注意点や他社の参考事例を盛り込み、より具体的で利用しやすい中小規模事業者向け資料**を作成する

（２）新たな研修会の実施

既存の研修※に加え、**関係省庁・団体とも連携し、**中小規模事業者における安全管理措置を推進させるための**新たな研修等を企画・実施**する

※　業界団体・中小企業関係等説明会開催実績　平成29年度　174回、　30年度　126回

情報収集

グッドプラクティス事例

２．「安全管理措置実態調査（オンサイトヒアリング）」の結果について

［本資料Ｐ３～４］

情報収集

中小企業における安全管理措置の実態及び当委員会への要望

３．「中小規模事業者の安全管理措置に関する実態調査（アンケート調査）」の報告結果について

［本資料Ｐ５～８］

情報収集

注意喚起が必要な事例

４．個人データの漏えい等事案を受けた対応

［本資料Ｐ９～10］