

(別添1)個人情報漏えい等に関する報告の記載要領

- 記入に際しては、「(別添1)個人情報漏えい等に関する報告(記載例)」を参照すること。
- 委託先が個人情報の漏えい等をした場合は、原則委託元が本報告を行うこと。
- 委託元の事業者は認定個人情報保護団体(以下、「認定団体」という。)の対象事業者ではないが、委託先の事業者が認定団体の対象事業者であり、かつ委託先の対象事業者が個人情報の漏えい等をした場合の対応については、委託元の事業者が経済産業省に本報告を行うとともに、委託先の対象事業者は所属する認定団体に連絡をすることが望ましい(認定団体からの経済産業省への報告は無し)。

(1)事業者名

漏えい等をした事業者名を記入する。委託先からの漏えい等の場合、委託元の事業者名を記入する。

漏えい等をした時点と現時点での事業者の名称が異なる場合、()に現時点の名称を記入する。

(2)分類

漏えい等が発生した部署について(参考)「日本標準産業分類(H14)」の中分類を記載。複数の分類にまたがる場合は、最も売上げが高い業種で分類する。

(3)発覚日

個人情報漏えい等したことが発覚した日付を記入する。(発生日と異なる場合が多いので注意する。)

(4)事案の概要(漏えい等の原因も含む)

漏えい等の原因を含めて、事案の概要を記入する。

(5)流出データの媒体、項目及び件数

[媒体(数)]

パソコン、顧客簿、USBメモリー等、及びその数を記入する。

[データ項目]

漏えい等をした個人情報の項目で、①～⑫で該当するものにチェックを入れる。その他の項目があれば、⑬の()内にすべて記入する。

[件数]

漏えい等の人数を記入する。未確定の人数があれば、()に記入する。

さらに、その人数を「顧客情報」「従業員情報」「その他の個人情報」の3つに分類する。

(6)暗号化等の情報保護措置

漏えい等をした個人情報電子媒体だった場合、暗号化等の措置の強弱に関わらず、何らかの措置が施されていたかどうかを記入する(ID・パスワードによる認証、生体認証等)。紙媒体が漏えい等をした場合は、なにも記入しないで下さい(措置無を選択する必要はない)。

*「一部措置有」とは、電子媒体と紙媒体の両方が漏えい等をした場合で、例えば、紛失したカバンの中に、閲覧する際にパスワードが必要なフロッピーディスクと、紙ファイルの顧客名簿が入っていた場合を指す。

(7)漏えい等に係る経緯

漏えい等が発生した日からの社内における主な動きについて、記入する。

*「発覚した経緯」「発覚してからの被害の拡大防止策」については、詳細に記入する。

(8)漏えい等元・漏えい等した者

[情報の漏えい等元]

当該事業者:①事業者の名称に記載されている事業者から個人情報が漏えい等をした場合。

委託先:①事業者の名称に記載されている事業者の委託先から個人情報が漏えい等をした場合。

不明:漏えい等の元が不明な場合。

[漏えい等をした者]

従業員(元従業員):(1)事業者の名称に記載されている事業者の従業員(元従業員)、または委託先の事業者の従業員(元従業員)が個人情報の漏えい等をした場合

第三者:(1)事業者の名称に記載されている事業者の外部の第三者が漏えい等をした場合。

不明:情報の漏えい等をした者が不明な場合。

* 事務所荒らしや車上荒らし等の盗難の場合は、「第三者」に分類する。

[意図的か不注意か]

意図的:漏えい等した者が「従業者(元従業者)」「第三者」によるもので、漏えい等が意図的なものである場合。

不注意:漏えい等した者が「従業者(元従業者)」「第三者」によるもので、漏えい等が不注意によるものである場合。

その他:天災、その他の理由によって個人情報漏えい等をした場合。

不明:意図的か不注意かによるものかが不明の場合。

* 事務所荒らしや車上荒らし等の第三者による盗難が漏えい等の原因である場合は、個人情報が主目的であるかどうかに関わらず、「意図的なもの」とする。

(9) 本人等への対応

[本人への連絡]

有:本人すべてに通知し、連絡がついた場合。

無:本人すべてに連絡がついていない場合。

* 謝罪の有無については、本項目では除外するものとする。

[その他の対応]

事業者が個人情報の漏えい等事案を受けて行った対応について、それぞれ、「関係者の処分」、「カード(銀行、クレジット等)の差し替え」、「専用窓口の設置」、「商品券等の配布」、「詫び状の送付(郵送・メール・FAX)」、「警察への届出(〇〇署)」として記入する。いずれにも該当しないものがある場合は、「その他」の()内に具体的に記入する。

* 戸別訪問による謝罪を行った場合は、「その他(戸別訪問による謝罪)」と記入する。

(10) 事案の公表

有:漏えい等の事案を自社のホームページに掲載したり、マスコミに対して公表した場合。

無:事案の公表を行わない場合は、()内にその理由を記入する。

(11) 2次被害

有:本人に2次被害が発生している場合は、詳細な内容を()内に記入する。本人から電話勧誘やダイレクトメールが増えた等の苦情があった場合も、本項目に記入する。

無:なにも2次被害が発生していない場合。

(12) 事業者による対応(再発防止策等)

漏えい等の事案をうけて、実施予定のものも含め、再発防止策について「組織的・人的安全管理措置」と「物理的・技術的安全管理措置」と区分して具体的な内容を記入する。

[組織的・人的安全管理措置]の例

- ・安全管理責任者、個人情報保護委員会等の設置
- ・個人情報保護に関する社内規定、プライバシーポリシー等の整備
- ・全社員、派遣社員、業務委託先を対象とする個人情報保護教育の実施
- ・定期的な内部監査・外部監査の実施
- ・委託先管理の強化(委託先の選定基準・管理基準の作成、定期検査の実施)

[物理的・技術的安全管理措置]の例

- ・外部とネットワーク接続している端末へのファイアウォールの構築
- ・アクセス権限認証の強化(生体認証機能導入)
- ・個人情報アクセス端末を対象に情報漏えい防止ソフトウェアを導入
- ・データ保存の暗号化、スクランブル化
- ・個人データへのアクセス状況の監視

(13) 報告先

[事業者から直接経済産業省に報告(月 日)]

認定団体を介さず、対象事業者が直接経済産業省に報告する場合に記入する。

[認定団体(〇〇団体)から経済産業省へ報告]

経済産業省に代えて、対象事業者が所属する認定団体に報告する場合に記入する。複数の認定団体に所属している場合は、経済産業省に報告する側の認定団体名を記入する。

[その他(〇〇省、〇〇県、認定団体△△組合)]

上記2つ以外の組織に報告を行う場合に、その組織名をすべて記入する。