

個人情報の取扱いに関する事故等の報告書

個人情報の取扱いに関する事故等（以下「事故等」という。）が発生しましたので、PMK500に基づき、報告いたします。

※代表印は不要ですが、必ず個人情報保護管理者に報告の済んだ状態でご提出ください。

17：[JUAS] 一般社団法人日本情報システム・ユーザー協会 宛

17：[JUAS] 一般社団法人日本情報システム・ユーザー協会 であることをご確認ください。

<注意事項>

該当する項目にチェックや記入を行って、原則、電子ファイルでご提出ください。

報告日：()

事故報告書の提出日をご入力ください。(再提出の場合は再提出日)
「報告日」に予め日付(22/03/15)が表示されている場合、PDFの作成方法に誤りがありますので、記入方法と提出方法の手順をご確認ください。

1. 報告種別

新規又は続報の別：—

前回報告日：()

速報又は確報の別：—

「続報」を選択した場合には、「前回報告日」をご入力ください。(2回目以降は「続報」)
「前回報告日」に予め日付(22/03/15)が表示されている場合、PDFの作成方法に誤りがありますので、記入方法と提出方法の手順をご確認ください。

3. 報告事項のPMK500 第12条第3項各号該当性「第1号～第5号」に該当しない場合は「速報」は不要です。

審査中(新規に限る)事業者、申請検討中事業者に該当する場合は、以下にチェック：

審査中事業者

申請検討中事業者

新規審査中・申請検討中事業者の場合は、選択してください。

2. 報告をする事業者の概要

事業者名称：()

登録番号※数字8桁：()

事業者所在地：()

代表者の氏名：()

報告者の氏名：()

報告者の所属：()

報告者の電話番号(ハイフン不要、数字のみ) ()

報告者のメールアドレス：()

事業者所在地の郵便番号の記入は不要です。報告者氏名は申請担当者以外でも可能です。本件事故の窓口となる方をご記入ください。

3. 報告事項

① 事態の概要

発生日：() 補足：()

発覚日：()

発生事象：

①漏えい

②紛失

「発覚日」に予め日付(22/03/30)が表示されている場合、PDFの作成方法に誤りがありますので、記入方法と提出方法の手順をご確認ください。

発生日が不明の場合は、発生したと思われる期間を「補足欄」にご記入ください。(例：YYYY/MM/DD～YYYY/MM/DD)

- ③滅失・き損
- ④改ざん、正確性の未確保
- ⑤不正・不適正取得
- ⑥目的外利用・提供
- ⑦不正利用
- ⑧開示等の求め等の拒否
- ⑨上記事象（－

①漏えい
 ②紛失（書類所在不明、スマートフォン紛失、書類誤廃棄など）
 ③滅失・き損（ランサムウェアによりデータ暗号化・消去されたなど）
 ④改ざん、正確性の未確保（アンケート調査結果改ざん、顧客情報誤登録など）
 ⑤不正・不適正取得（同意なく個人情報を取得したなど）
 ⑥目的外利用・提供（配信停止の人にメルマガを配信したなど）
 ⑦不正利用（業務で知り得た顧客情報の不正利用など）
 ⑧開示等の求め等の拒否（正当な理由なく個人情報の開示請求に応じないなど）
 ⑨上記事象のおそれ（誤送付された書類が未開封で戻ってきた、紛失した書類が見つかったなど）

※事象のおそれが複数ある場合には、最も該当する事象をご選択ください。

- 発見者：当社
委託元
委託先
取引先
顧客／会員
カード会社／決済代行会社
その他（

事故等の発見者をご選択ください。
 事故の発見者とは、事故が発生したことを認識した人です。

PMK500第12条第3項各号該当性

- 第1号（要配慮個人情報）
要配慮個人情報が含まれる事故等
- 第2号（財産的被害）
財産的被害が生じるおそれがある事故等
- 第3号（不正の目的）
不正の目的をもって行われたおそれがある事故等
- 第4号（千人超）
個人データにかかる本人の数が千人を超える事故等
- 第5号（個人情報の取扱いルールの重大な違反、又はそのおそれ）
その他、プライバシーマーク付与適格性審査基準における重大な違反

こちらのチェックは必須ではありません。
 速報対象の事故の場合には、項目をご選択ください。
 （複数選択可）
 速報対象の事故でない場合はチェックは不要です。

本件は受託業務における事故であるか：－
 ※○の場合は以下の項目を記入ください

- 委託元名称：（
- 委託元のPマークの取得：－
- 委託元住所：（
- 委託元電話番号（ハイフン不要、数字のみ）：（

委託元・委託先がPマーク付与事業者でない場合でも事故の状況を詳細に把握するためにご記入をお願いいたします。
 （必須ではありません）

本件は委託先が関連する事故であるか：－
 ※○の場合は以下の項目を記入ください

- 委託先名称：（
- 委託先のPマークの取得：－
- 委託先住所：（
- 委託先電話番号（ハイフン不要、数字のみ）：（

※複数に委託している場合、委託先の名称、Pマーク取得の有無、委託先の住所、委託先の電話番号を記載
委託先が複数の場合2社目以降を記載：

[]

事実経過を以下にできるだけ詳細に記載ください。

事故の概要をできるだけ詳細にご記入ください。

(1) 事実概要：

例1.
弊社の事務職員がテレワーク時に、顧客情報データの入力を行うため、事前にUSB（従業員私用）に顧客データを保存し、帰宅途中に紛失した。

例2.
弊社が運営するショッピングサイト「〇〇」（オープンソースのECサイト構築用プログラムで構築 ※製品名、バージョン情報等詳細をご記入ください）がXSS攻撃による不正アクセスを受けクレジットカード情報が漏えいした。

(2) 事故が発生した事業（サービス）の概要：

事故が発生したサービス名・事業概要や業務フローを具体的にご記入ください。

例1.ヘアケア商品を販売するECサイト「●●」事業
例2.クレジットカード事業の加盟店向け店頭決済サービス「●●」

(3) 発覚の経緯・発生後の事実経過（時系列）：

例：
20●●年3月28日 従業員Aがテレワークで入力作業を行うため、無断で顧客情報を私用USBに保存し自宅に持ち帰った。
20●●年3月29日 従業員Aがテレワークで入力作業を行うため、USBを使用する際に、紛失していることが発覚。
20●●年3月29日 従業員Aが会社に出社し、上席に紛失を報告。
帰宅途中に立ち寄った経路を搜索したが、発見できなかった。
20●●年3月29日 鉄道会社や警察署へ遺失物届を提出。
20●●年3月29日 会社ホームページで公表
20●●年3月30日 通行人より警察署に届け出があり発見

発生・発覚からの事実関係及び対応経緯、また、事故を公表した場合は公表に至る経緯を時系列でご記入ください。（5W1Hを示して具体的にご記入をお願いします。）
また、事故対象の個人情報の媒体が発見、回収された場合は、その旨記入してください。

(4) 外部機関による調査の実施状況：

外部機関による調査を実施している場合に詳細をご記入ください。
調査を検討中、予定がない場合にはご選択ください。

外部機関調査実施済（実施中）

依頼日：（ ） 完了日（完了予定日）：（ ）

外部機関調査実施予定

依頼予定日：（ ） 補足：（ ）

外部機関調査検討中

外部機関調査予定なし

※外部機関名、調査概要などの実施状況などは以下に記載

外部機関調査詳細：

()

不正アクセス等で外部機関調査（フォレンジック調査）を行っている場合には、外部調査機関名や、調査概要・結果等をご記入ください。

② 事故等が発生、又は発生したおそれがある個人情報の項目

媒体：紙

電子データ

その他

()

口頭による漏えいの場合、「口頭（対面）」「口頭（電話）」のようにその他欄にご記入ください。

人数：顧客情報

と 人数 ※数字のみ：（ ） 補足：（ ）

種類 うちクレジットカード情報を含む人数※数字のみ：（ ）

補足：（ ）

従業者情報

人数 ※数字のみ：（ ） 補足：（ ）

その他

人数 ※数字のみ：（ ） 補足：（ ）

合計人数※自動反映：（ 0 ） 補足：（ ）

人数は必ず記入。不明の場合でもわかる範囲で概算数を記入のこと。(数字は半角)

項目：氏名

生年月日

性別

住所

電話番号

メールアドレス

口座番号

(銀行印印影)

取引(利用)情報、購入履歴等

事故等が発生又は発生のおそれがある個人情報の人数を顧客情報（消費者）、従業員、その他に分けてご記入ください。
※取引先情報は「その他」に記入してください。
※合計人数は自動計算されます。

- マイナンバー
- 実印印影
- 匿名加工情報の加工方法等情報
- 会員 ID
- パスワード
- 家族に関する情報
 - 家族に関する情報の具体的項目：()
- 健康に関する情報
 - 健康に関する情報の具体的項目：()
- 収入・資産・債務情報
 - 収入・資産・債務情報の具体的項目：()
- クレジットカード情報
 - (クレジットカード番号、有効期限、セキュリティコード)
- その他・補足

事故等が発生又は発生のおそれがある個人情報の項目を選択してください。

()

③ 発生事象の詳細

主体：

- 報告者
- 委託先
- 配送委託先
- 不明

事故発生事象における当事者をご選択ください。

事象分類：

- 誤送信（メール、SMS、メッセージ等）
- 誤配達・誤交付（配送物、文書・カードなどの手渡し等）
- 誤廃棄
- 紛失・滅失・き損
- 盗難
- 誤表示（webサイト、掲示板等）
- 誤登録（システムへの登録等）
- 内部不正行為
- 不正アクセス
- マルウェア・ウイルス 名称：()

■ 誤送信：目的外利用・提供に含まれる事故（配信停止の人にメルマガが配信されたなど）は誤送信を選択してください。
■ 誤表示：誤った情報が第三者に閲覧可能な状態になること
■ 誤登録：データの入力間違い
■ 内部不正行為：従業員が悪意を持って不正行為を行った場合
■ マルウェア・ウイルス」名称：
「マルウェア・ウイルス」等の名称が明らかな場合には、ご記入ください。（エモテット・ランサムウェア等）
※複数選択可能です。
例. システムの誤登録により誤送信となった場合には、誤送信および誤登録にチェックしてください。

原因分類：（複数選択可能）

<担当者>

作業、操作ミス

← 人的なうっかりミス

定められた手順、ルールに反した作業、操作

← 担当者が定められたルールに意図して従わずに作業を行った

<確認者>

確認不足

← 人的なうっかりミス

定められた手順、ルールに反した確認

← 担当者が定められたルールに意図して従わずに確認を行った

<組織（事業者、部署、グループなど）>

定められた手順、ルールが不明瞭又は手順、ルールの未策定

従業員への教育が不十分

リスクの特定、分析及び評価が不十分

安全管理措置の不備

簡易なパスワード設定

アクセス制御の不備（入退出管理含む）

プログラムの設計、設定の不備

バージョンアップ、セキュリティパッチの適用の不備

SQL インジェクション対策の不備

クロスサイトスクリプティング対策の不備

パスワードの平文保持

その他

(

)

原因の詳細：

← 事故発生の直接的及び根本的な原因・問題点をご記入ください。

例.

[直接的な原因]

メルマガを配信する際に、担当者が誤ってBCCをCCに設定して送信してしまった。送信前にダブルチェックを行ったが、見落とししてしまった。

[根本的な原因]

- ・メルマガ配信の際の手順をルール化をしていなかった。
- ・送信前のダブルチェックの際に確認手順・項目を明確に定めていなかった。
- ・個人情報を取り扱う教育が不十分であった。

※不正アクセスの場合には、詳細原因、手法（脆弱性箇所、攻撃手法（SQLインジェクション、マルウェア、リスト型、）、システムの管理状況（委託先や自社開発）、アンチウイルスソフトの使用状況を記載してください。

④ 安全管理措置

安全管理措置：

暗号化

対象：(

)

匿名化

対象：(

)

← 安全管理措置の対応についてご選択及びご記入ください。

- 仮名化
対象:()
- パスワード保護
対象:()
- その他
()
- 措置なし
- 不明

二次被害又はそのおそれの有無及びその内容をご回答ください。

- ⑤ 二次被害又はそのおそれの有無及びその内容
二次被害又はそのおそれの有無：－
上記に関する事故後の対応：－
詳細:()
※具体的な内容を詳細に記載してください

本人への対応の実施状況をご回答ください。

- ⑥ 本人への対応の実施状況
本人への対応（通知含む）：－
詳細:()
※ 実施日、実施予定日や対応予定なしの場合はその理由を具体的な内容を詳細に記載

事故等の公表（メディアやホームページ等(社外)に対して)の実施状況をご回答ください。

- ⑦ 公表の実施状況
事案の公表：
 実施済
公表日:() 補足:()
 公表予定
公表予定日:() 補足:()
 検討中
 予定なし（理由：)
公表の方法：
 ホームページに掲載
 記者会見
 報道機関等への資料配布
 その他 ()

公表文等の詳細：※公表文やホームページ記載の URL 等を記述ください。

[]

⑧ 再発防止のための措置

実施済の措置：



今後実施予定の措置及び完



※長期的に講ずる措置を含む

組織的・人的・物理的・技術的安全管理措置の観点でご記入ください。

- 組織的安全管理措置
安全管理についての従業員の責任と権限を明確に定め、安全管理に対する規定や手順書を整備運用し、その実施状況を確認すること。
- 人的安全管理措置
従業員に対する業務上秘密と指定された個人情報の非開示契約の締結や教育・訓練等を行うこと。
- 物理的安全管理措置
入退室（館）管理、個人情報の盗難の防止等の物理的な安全管理措置。
- 技術的安全管理措置
個人情報を取り扱う情報システムへのアクセス制御、不正アクセス制御、不正アクセスソフトウェア対策、情報システムの監視、個人情報に対する技術的な安全管理措置

⑨ その他

その他参考となる事項があれば記載：←

その他共有・補足事項がある場合にご記入ください。



自社がJIPDEC認定個人情報保護団体対象事業者かどうかの確認は、JIPDECホームページ「認定個人情報保護団体対象事業者検索」をご参照ください。

⑩ 当方以外への報告について

JIPDEC 認定個人情報保護団体対象事業者ですか：－

他に対象事業者となっている認定個人情報保護団体があれば記載ください：

()

JUASかどうかの確認は、JUASホームページ「認定個人情報保護団体対象事業者一覧」をご参照ください。

個人情報保護委員会への報告は完了していますか：－

詳細（報告実施日・予定日を記載）：()

事業所管大臣への報告は完了していますか：－

詳細（権限が委任された府省庁、報告実施日・予定日を記載）：

()

委託元への報告は完了していますか：－

詳細（報告実施日、予定日を記載）：()

その他関係機関（警察、IPA、JPCERT/CC 等）への報告は完了していますか：－

詳細（報告先・報告実施日・予定日を記載）：

()

記載要領

1. 2. の「報告者の氏名」の「電話」には、代表電話番号ではなく、当該事務連絡者の直通電話番号を記載すること。
2. 3. ⑦の「公表文等の詳細」には、公表を予定している場合、公表予定の文案を記載又は添付すること。
3. JIPDECの認定個人情報保護団体対象事業者は、「JIPDEC 個人情報保護指針」に基づき、JIPDECの認定個人情報保護団体にも本事故報告書は共有します。
4. JUASの認定個人情報保護団体対象事業者は、「JUAS個人情報保護指針」に基づき、JUASの認定個人情報保護団体にも本事故報告書は共有します。