情報セキュリティインシデントに関する調査報告書

別紙

第 1.0 版

NPO 日本ネットワークセキュリティ協会
セキュリティ被害調査ワーキンググループ

© Copyright 2017 NPO Japan Network Security Association (JNSA)

目次

著作権・引用について

本報告書は、NPO 日本ネットワークセキュリティ協会(JNSA) セキュリティ被害調査ワーキンググループが作成したものである。著作権は当該 NPO に属するが、本報告書は公開情報として提供される。ただし、全文、一部にかかわらず引用される場合は、「(引用) JNSA 情報セキュリティインシデントに関する調査報告書別紙」と記述して欲しい。なお、報告書の文書を改変して使用する、あるいは報告書内の集計データを独自に再編して新たなグラフを作成するなど、報告書内の情報を加工して使用する場合は「引用」ではなく「参考」と表記していただきたい。また、書籍、雑誌、セミナー資料などに引用される場合は、JNSA のホームページ上にある問い合わせフォームをご利用ください。

改訂履歴

版数	発行日	改訂内容
第 1.0 版	2017 年 5 月 17 日	初版発行

© Copyright 2017 NPO Japan Network Security Association (JNSA)

1　想定損害賠償額の算出の目的

想定損害賠償額の算定式の提案、及び算出式を実際のインシデントに適用した想定損害賠償額の算出は、当ワーキンググループの調査報告書の特徴である。

当ワーキンググループは、当初から実際に発生したインシデントの分析によるリスクの定量化と対策効果の定量化を目的に活動してきた。想定損害賠償額算定式の提案も、個人情報を取り扱う組織の潜在的なリスクを数値として把握することを目的にしている。よって、本算定式は各組織が所有する個人情報の潜在的リスクを把握するためのひとつの推定方法であり、被害者が漏えい元の組織に対して請求できる損害賠償額を示したものではない点を認識いただきたい。また、個人情報を保有している組織は、保有する個人情報について算定を試みていただきたい。

なお、以下に挙げる算定結果は、あくまでも「もし被害者全員が賠償請求したら」という“仮定”に基づくものであり、実際に各事例においてその金額が支払われたものではないことに注意していただきたい。

2　想定損害賠償額算定式の解説

想定損害賠償額の算定にあたっては、2015 年も 2003 年の調査方法を踏襲した。改定を行わなかった理由は、現実の判決による賠償額と本算定式による算定結果が許容できる範囲の差異に収まったことから、現行の算定式が十分使えるものと判断したためである。

想定損害賠償額の算定式の成り立ちについては、2003 年の報告書を参照いただきたい。ここでは簡単に概要を記述するに留める。想定損害賠償算定式の策定プロセスは図 2-1 に示す通りである。

2.1　想定損害賠償額算定式の策定プロセス

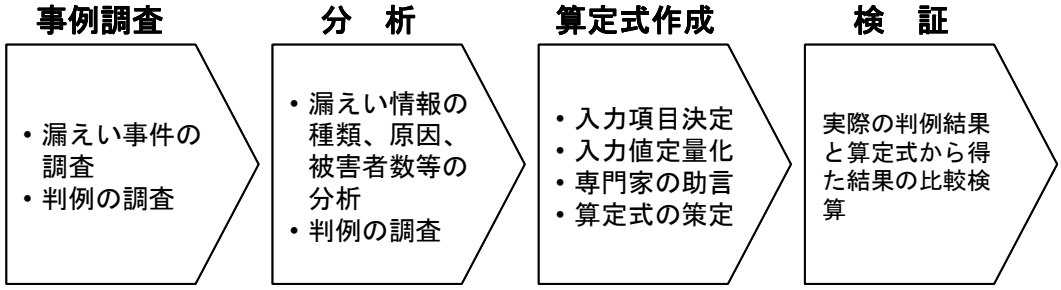

図 2-1：想定損害賠償額算定式策定のプロセス

© Copyright 2017 NPO Japan Network Security Association (JNSA)

① 事前調査

報道されたインシデントを調査・集計する。同時に過去のプライバシー権侵害や名誉毀損の判例を調査する。ここでは 2003 年の報告書で説明した通り、「宇治市住民基本台帳データ大量漏えい事件控訴審判決 大阪高等裁判所平成 13 年（ネ）第 1165 号 損害賠償請求控訴事件」を参考にした。

② 分析

集計したインシデントの被害者数、漏えい情報種別、漏えい原因、漏えい経路などを分析する。

③ 算出式作成

算出式の入力項目を決定し、算定式を策定。入力項目は、漏えい情報の価値、漏えい組織の社会的責任度、事後対応評価とした。また、弁護士など専門家の意見も取り入れた。

④ 検証

策定した算定式の信憑性をはかるため、先の宇治市の事例に当てはめ、算定式で得られた結果と実際の判決による損害賠償額と比較した。Yahoo! BB、及び TBC の判決との比較も行った。その結果、同程度の数値が得られた。

2.2 算定式の入力値の解説

当該算定式では以下の項目を入力値とした。

- **漏えい個人情報価値**
- **情報漏えい元組織の社会的責任度**
- **事後対応評価**

実際の訴訟では、これらの項目以外にも、事前の保護対策状況、漏えいした情報の量、漏えい後の実被害の有無、事後対応の具体的な内容なども評価されると考えられる。しかし、当該算定式の策定において参考にする情報は公開情報であり、そこから読み取れる内容には限りがある。また、入力値や算出方法が複雑すぎて、セキュリティの専門家でなければ計算できなかったり、算出に必要な入力値が収集できなかったりすると、各組織が自ら所有する個人情報の潜在的リスクを算出するという目的に用いられなくなってしまう。よって、入力値をこれらに絞り、かつ値の算定が容易となるような計算方法を策定した。

以下に、それぞれの入力値を定量化して想定損害賠償額を算定する方法を解説する。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

(1)　漏えい個人情報の価値

個人情報が漏えいした際に被害者に与える影響を、「経済的損失」と「精神的苦痛」という 2 種類の尺度で分類した。影響の大きさを定量化するため、縦軸（y 軸）に「経済的損失」の度合いを、横軸（x 軸）に「精神的苦痛」の度合いを持たせたグラフを作成した。このグラフを便宜上 EP 図（Economic-Privacy Map）と名づける（図 2-2）。x 軸の正の方向の位置によって精神的苦痛の大きさを、y 軸の正の方向の位置によって経済的損失の大きさを表現する。

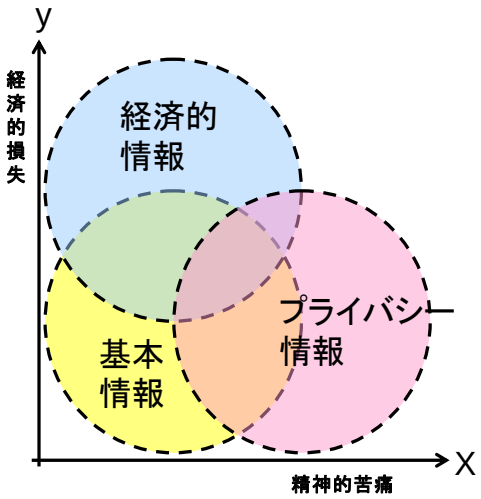

図 2-2：EP 図（Economic-Privacy Map）

この EP 図上へ、「個人情報の保護に関する法律（個人情報保護法）」、「個人情報保護マネジメントシステム－要求事項（JIS Q 15001）」、及び過去の情報漏えいインシデントの調査分析で得られた漏えい情報の種類をプロットした。漏えいした情報がどのような影響をあたえるのか、つまり EP 図上の情報の位置により情報の価値を求めることができる。さらに、算出式への値の入力のしやすさ等を考慮し、EP 図の x 軸、及び y 軸をそれぞれ 3 段階に分け、漏えい情報の影響の度合いに応じて、漏えい情報を種類別に再配置した。再配置した図 2-3 が、シンプル EP 図である。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

経済的損失レベル				
	3	口座番号＆暗証番号、クレジットカード番号＆カード有効期限、金融系Webサイトのログインアカウント＆パスワード、決済機能付きのサイトの顧客登録情報（アカウントにメールアドレスを使用する場合も含む。）	遺言書	前科前歴、犯罪歴、与信ブラックリスト
	2	パスポート情報、購入記録、ISPのアカウント＆パスワード(アカウントにメールアドレスを使用する場合も含む。決済機能のないサイトのアカウント＆パスワードも含む)、口座番号のみ、クレジットカード番号のみ、金融系Webサイトのログインアカウントのみ、印鑑登録証明書、ソーシャルセキュリティナンバー、サービス申込(加入申請)情報	年収・年収区分、所得、資産(固定資産税など)、建物、土地、残高、借金、所得(生活保護に関わる情報含む)、借り入れ記録、購入履歴(スタンプやポイントは除く)、給与額、賞与額、納税金額、寄付目的・金額、税や保険、保育費などの未納金額	
	1	氏名、住所、生年月日、性別、金融機関名、住民票コード、メールアドレス、健康保険証番号、年金証書番号、免許証番号、社員番号、会員番号、電話番号、ハンドル名、健康保険証情報、年金証書情報、介護保険証情報、会社名、学校名、役職、職業、職種、身長、体重、血液型、身体特性、写真、肖像、音声、声紋、体力測定値、家族構成、ISPアカウント名のみ、患者番号、受診科目・受診日、水栓番号、保険加入状況に関する情報、請求に係る金額(払戻しの請求金額など)	健康診断結果(結核検査記録など)、心理テスト結果、性格判断結果、病歴、手術歴、妊娠歴、看護記録、その他身体検査記録、治療法(治療に係る記録映像含む)、レセプト情報(治療に係る金額)、身体障がい者手帳情報、DNA情報、身体障がい情報、知的障がい情報、指紋、生体認証情報(静脈,声紋,虹彩,網膜,顔画像等)、スリーサイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、賞罰(交通違反切符など)、職歴(求職に関する書類含む)、学歴(求職に関する書類含む)、成績(教務手帳を含む)、試験得点(解答用紙など含む)、日記、メール内容(内容によって、どの情報に該当するかを判断すべし)、位置情報、児童相談に関わる情報、高齢者医療保険や介護保険の還付金額、プライベート(恋愛)情報	加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍(戸籍附票、住民票に記載される本籍も含む)、病状(結核医療に関する情報など)、保有感染症、カルテ(エックス線写真も含む)、認知症情報、精神的障がい情報、性癖、性生活の情報、介護度、プライベート(不倫)情報(写真も含む)
		1	2	3
				精神的苦痛レベル

図 2-3：シンプル EP 図

ただし、単純に情報をシンプル EP 図上にあてはめて、その座標値（x 値、y 値）から漏えい情報の価値を推定するのではなく、実被害への結び付き易さを考慮して補正を加える必要があると考えた。その補正を加えた漏えい情報の価値を求めるための算出式を以下に示す。

漏えい個人情報価値 ＝ 基礎情報価値×機微情報度×本人特定容易度

© Copyright 2017 NPO Japan Network Security Association (JNSA)

各属性値の定義は、以下の通りである。

a. 基礎情報価値

基礎情報価値には、情報の種類に関わらず基礎値として、“一律 500 ポイント”を与えることとした。

b. 機微情報度

一般的に機微情報(センシティブ情報)とは、思想・信条や社会的差別の原因となる個人的な情報など、JIS Q 15001 で収集禁止の個人情報として定義されるような一部の情報に限定されることが多い。しかしこれら以外の情報でも精神的苦痛を感じる場合がある。本算出式では個人情報全体に対して 3 段階のレベルを設定し、その値からセンシティブの度合いを算定できるよう定義した。また経済的損害を被る情報についても機微情報度の算出式に含めた。

機微情報度は、対象となる情報のシンプル EP 図上の（x, y）の位置（=レベル値）を下記の式に代入して求める。

$$\text{機微情報度} = (10^{x-1}+5^{y-1})$$

漏えい情報が複数種類ある場合は、全情報のうちで最も大きな x の値と最も大きな y の値を採用する。例えば「氏名、住所、生年月日、性別、電話番号、病名、口座番号」が漏えいした場合、シンプル EP 図上の（x, y）は以下のようになる。

$$\text{「氏名、住所、生年月日、性別、電話番号」} = (1, 1)$$
$$\text{「病名」} = (2, 1)$$
$$\text{「口座番号」} = (1, 3)$$

この例で最も大きい x 値は病名の“2”であり、最も大きい y 値は口座番号の“3”である。これらの値を前述の数式に当てはめると以下のようになる。

$$(10^{2-1}+5^{3-1}) = (10^{1}+5^{2}) = 35\text{ポイント}$$

c. 本人特定容易度

本人特定容易度は、漏えいした個人情報からの本人特定のし易さを表すものである。例えば銀行の口座番号が単独で漏えいしても、氏名などの本人を特定する情報が伴わなければ実被害に結び付きにくいことから、本人特定容易度を本算出式に含めた。本人特定容易度は、以下の表 2-1 に示す判定基準を適用する。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

表 2-1：本人特定容易度 判定基準

判定基準	本人特定容易度
個人を簡単に特定可能。 「氏名」「住所」が含まれること。	6
コストをかければ個人が特定できる。 「氏名」または「住所 ＋ 電話番号」が含まれること。	3
特定困難。上記以外。	1

(2) 情報漏えい元組織の社会的責任度

社会的責任度は表 2-2 に示すように、「一般より高い」と「一般的」の 2 つから選択する。社会的責任度が一般より高い組織は、「個人情報の保護に関する基本方針(平成 16 年 4 月 2 日 閣議決定)」に「適正な取り扱いを確保すべき個別分野」として挙げられている業種を基準とし、そこへ政府機関など公的機関と知名度の高い大企業を含めることとした。

表 2-2：情報漏えい元組織の社会的責任度 判定基準

判定基準		社会的責任度
一般より高い	個人情報の適正な取り扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信など）、及び公的機関、知名度の高い大企業。	2
一般的	その他一般的な企業、及び団体、組織	1

© Copyright 2017 NPO Japan Network Security Association (JNSA)

(3) 事後対応評価

表 2-3 に基づいて、事後対応の評価値を求める。事後対応が「不明、その他」の場合、不適切な事後対応が露見しなかったと考え、適切な対応が行われた場合と同じ値とした。

表 2-3：事後対応評価 判定基準

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

事後対応を評価する明確な基準がないため、過去の情報漏えいインシデントにおける事後対応行動を参考に作成した表 2-4 の対応行動例にあてはめて、事後対応の適切／不適切を判断する。

表 2-4：事後対応 行動例

適切な対応行動例	不適切な対応行動例
すばやい対応	指摘されても放置したままである
被害状況の把握	対応が遅い
インシデントの公表	繰り返し発生させている
状況の逐次公開(ホームページ、メール、文書)	対策を施したが、有効でない
被害者に対する事実周知、謝罪	虚偽報告
被害者に対する謝罪(金券の進呈を含む)	
顧客に与えるであろう影響の予測	
クレーム窓口の設置	
漏えい情報回収の努力	
通報者への通報のお礼と顛末の報告	
顧客に対する補償	
経営者の参加による体制の整備	
原因の追究	
セキュリティ対策の改善	
各種手順の見直し	
専門家による適合性の見直し	
外部専門家の参加による助言や監査の実施	

© Copyright 2017 NPO Japan Network Security Association (JNSA)

2.3　想定損害賠償額算出式

以上の定量化した「漏えい個人情報価値」、「情報漏えい元組織の社会的責任度」、「事後対応評価」の値を以下の算定式に代入することによって、想定損害賠償額が算出できる。算出式の全体像を図 2-4 に示す。

想定損害賠償額 ＝ 漏えい個人情報価値
× 情報漏えい元組織の社会的責任度
× 事後対応評価

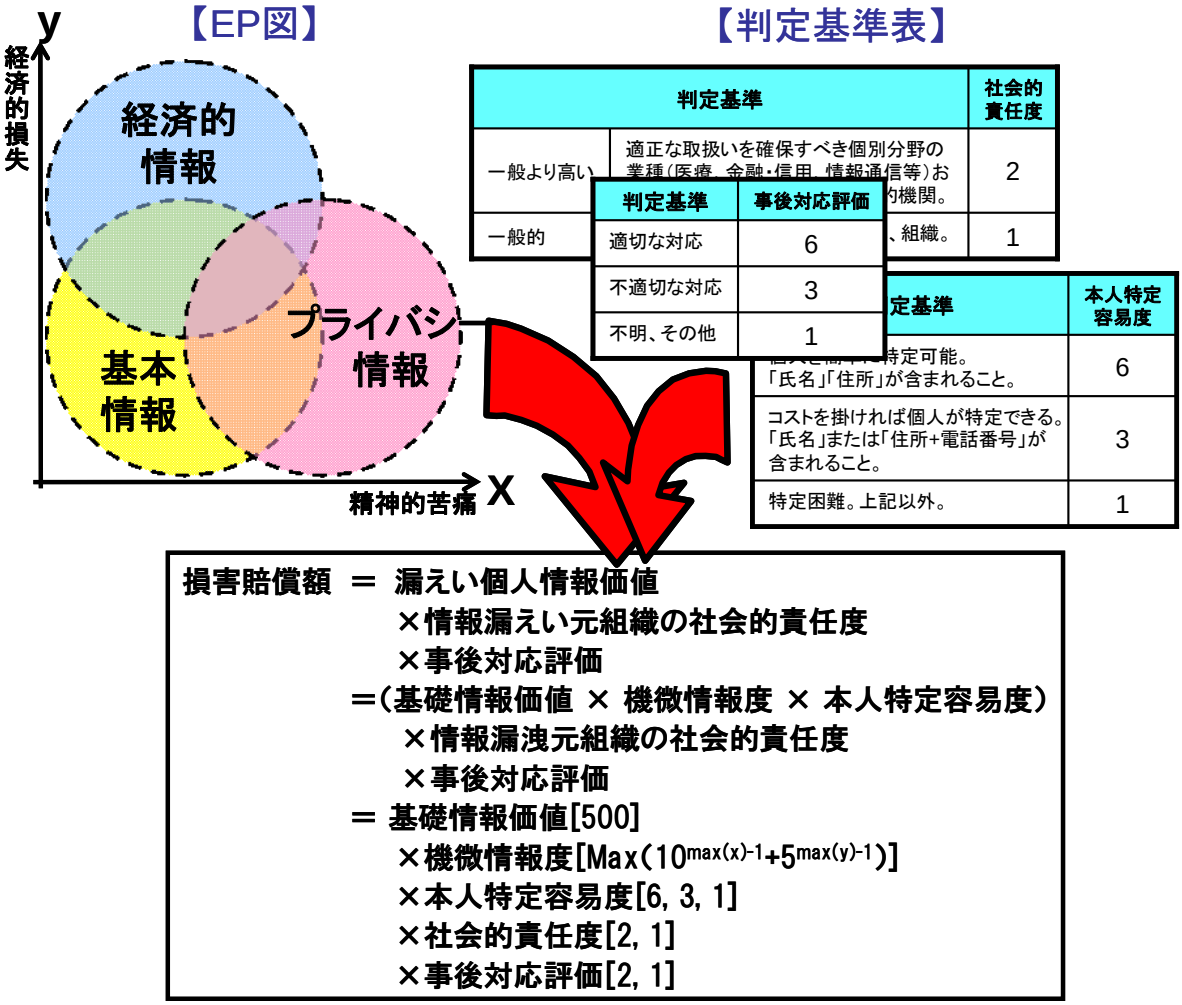

図 2-4：JO モデル

上記の想定損害賠償額算出式を、当ワーキンググループでは JO モデル（JNSA Damage Operation Model for Individual Information Leak）と名付けた。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

3　一人あたりの平均想定損害賠償額について

「一人あたりの想定損害賠償額」は、インシデント毎に算出している。「一人あたりの平均想定損害賠償額」は、このインシデント毎の「一人あたりの想定損害賠償額」の平均金額を求めた。よって、全インシデントの「一人あたりの想定損害賠償額」を合計し、「インシデント総件数」で除算して、「一人あたりの平均想定損害賠償額」を算出している。「想定損害賠償額の合計」を「漏えい人数の合計」で、除算した値ではないことに注意されたい。

算出式、及び具体的な計算例は、以下の通りである。

インシデントが以下の 2 件の場合
A インシデントの一人あたり想定賠償額 ＝a 円
B インシデントの一人あたり想定賠償額 ＝b 円
一人あたりの平均想定損害賠償額 ＝(a 円＋b 円)÷2 件

■具体例

表 3-1：インシデント内容（具体例）

	漏えい人数	想定損害賠償総額	一人あたりの 想定損害賠償額
A インシデント	1 人	100 万円	100 万円
B インシデント	100 人	100 万円	1 万円

表 3-2：一人あたりの想定損害賠償額（具体例）

	漏えい人数	一人あたりの想定損害賠償額
人数で除算した場合	101 人	200 万円÷101 人 ＝1.98 万円
本報告書の場合	101 人	(100 万円+1 万円)÷2 件 ＝50.5 万円

© Copyright 2017 NPO Japan Network Security Association (JNSA)

4　漏えい原因の定義

漏えい原因は以下のように分類した。

表 3：漏えい原因区分の考え方

原因区分	具体的事象例	判断基準
設定ミス	Web 等の設定ミスにより外部から閲覧できる状態になっていて、機密情報が閲覧された可能性がある。	ユーザが Web サーバやファイルのアクセス権などの設定を誤ったことよって情報が漏えいした場合。 ※　この設定ミスを悪用して、故意に情報を盗んだとしても、不正アクセスには分類しない。 ※　ソフトウェアの脆弱性ではないため、バグ・セキュリティホールには分類しない ※　情報の管理手順上の手落ちによる漏えいは管理ミスに分類する。
誤操作	あて先間違いによって、電子メール・FAX・郵便の誤送信が発生した。	あて先を書き間違えたり、操作ボタンを間違えて押したりするなどの人間のオペレーションによって情報が漏えいした場合。 ※　最終的なオペレーション段階によるミスを誤操作とする。メール配信システムの設定が間違っていた場合には設定ミスに分類する。
バグ・セキュリティホール	OS、アプリケーション等のバグ・セキュリティホールなどにより、Web 等から機密情報が閲覧可能、または漏えいした。	OS やアプリケーション等の既存ソフトウェア上のバグ・セキュリティホールが原因で情報が漏えいした場合。 ※　ユーザ側でバグ・セキュリティホールが放置されていた場合も含む。 ※　ソフトウェアベンダーやシステムベンダーによる対処がされていなかった場合も含む
不正アクセス	ネットワークを経由して、アクセス制御を破って侵入され、機密情報が外部に漏えいした。	外部の第三者が、主にネットワークを経由して不正にアクセスを行って情報が漏えいした場合。 従業者・使用人など内部の人間の不正アクセスの場合は、内部犯罪・不正行為に分類する。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

原因区分	具体的事象例	判断基準
内部犯罪・内部不正行為	社員・派遣社員など内部の人間が、機密情報を悪用するために不正に取得して持ち出した。持ち出した情報を使って犯罪を行ったり、売買したりして、漏えいした。	社員、管理下にある他社社員(派遣社員など)が、不正アクセス、その他不正な行為によって情報を持ち出して悪用した場合。 ※ 外部の人間との結託や不正アクセスを伴う場合も、内部の人間の積極的な不正行為があれば内部犯罪・不正行為に分類する。 ※ 業務上の必要性などから、ルールを逸脱して情報を持ち出した場合は、不正な情報持ち出しに分類する。
不正な情報持ち出し	社員、派遣社員、外部委託業者、出入り業者、元社員などが、顧客先、自宅などで使用するために情報を持ち出して、持ち出し先から漏えいした。	業務上の必要性などから、ルールを逸脱して情報を持ち出した場合。ただし、ルールを逸脱して情報や情報媒体を持ち出した場合、厳密には盗難であるが、左記のような場合は情報持ち出しとする。 ※ 社員がルールを逸脱して機密情報を自宅に持ち帰り、ファイル交換ソフト経由で漏えいした場合も、不正な情報持ち出しに分類する。
目的外使用	組織ぐるみ、もしくは組織の業務に関連して、個人情報を目的以外の用途で使用した。関係会社など、開示範囲外の組織に公開した。	個人情報を当初の目的以外の用途に使用した場合。開示範囲外を越えて公開した場合。 ※ 社員、派遣社員などの内部の人間が、個人的に個人情報を目的外使用した場合は、内部犯罪・内部不正行為に分類する。
紛失・置忘れ	電車、飲食店など外部の場所に、PC、情報媒体等を紛失または置忘れてしまった。	持ち出し許可を得た情報を、持ち出し先や移動中に置忘れたり、紛失したりした場合。個人の管理ミスによって発生した場合。 ※ 社内において、管理すべき情報を紛失した場合は、管理ミスに分類する。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

原因区分	具体的事象例	判断基準
盗難	車上荒らし、事務所荒らしなどにより、PC 等の情報媒体とともに機密情報が盗難された。	第三者によって情報記録媒体と共に情報が盗まれた場合。車上荒らし、事務所荒らしなど。 ※ 情報のみ盗難された場合は、不正アクセスに分類する。
管理ミス	引越し後に個人情報の行方がわからなくなった。 個人情報の受け渡し確認が不十分で、受け取ったはずの個人情報が紛失した。 情報の公開、管理ルールが明確化されておらず、誤って開示してしまった。	社内や主要な流通経由において紛失・行方不明となった場合。作業手順の誤りや、情報の公開、管理ルールが明確化されていなかったために業務上において漏えいした場合。紛失の責任が組織にある場合。 ※ 管理ミスによって盗難が発生した場合は、盗難に分類する。 ※ 社内において、管理が行き届かずに誤って破棄した場合も含む。
ワーム・ウイルス	ワームの感染により、意図に反してメールが発信されてしまい、メールアドレス等の個人情報が漏えいした。	ウイルス・ワームによって、情報が漏えいした場合。原因そのものがワームによる場合は、ワーム・ウイルスとする。 ※ セキュリティホール等を利用したウイルス、ワームによって、情報が漏えいした場合も含む。 ※ ファイル交換ソフトにウイルス・ワームが感染して情報が漏えいした場合、自宅に情報を持ち帰るなどの不正な情報持ち出しや社内の PC でファイル交換ソフトを使用するなどの管理ミスが原因ではない場合はワーム・ウイルスに分類する。
その他	ダイレクトメール封入時に他人宛の文書も混入してしまった。	上記のいずれにも該当しないもの。
不明		原因が不明なもの。

© Copyright 2017 NPO Japan Network Security Association (JNSA)

5　お問い合わせ先

本報告書に関する引用・内容についてのご質問等は JNSA ウェブサイト上の引用連絡およびお問合せフォームからご連絡下さい。

※引用のご連絡に対する承諾通知はご返信しておりませんのでご了承下さい。

また報告書についての FAQ もございますので、引用・お問合せの際はご参照下さい。

http://www.jnsa.org/faq/incident.html

■お問い合わせフォーム

引用連絡および問合せフォーム

URL： https://www.jnsa.org/aboutus/quote.html

© Copyright 2017 NPO Japan Network Security Association (JNSA)