【巻末別表】

本文 第 16 条規程の「個人情報漏えい等の事故への対応」を次のとおり実施するものとする。

＞＞ 行政報告要領及び本人への通知要領の詳細 ＜＜

■「漏えい」「滅失」「毀損」の意味

個人データの「漏えい」「滅失」「毀損」（総称して「漏えい等」）の意味について、ガイドラインでは次のように記述されています。ただし、当該個人データに関して、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告不要とされています。なお、漏えい等の「おそれ」がある場合とは、漏えい等が疑われるが漏えい等があったことの確証がない場合をいいます。

漏えい ➔

個人データが外部に流出すること。

事例 1）個人データが記載された書類を第三者に誤送付した
事例 2）個人データを含むメールを第三者に誤送信した
事例 3）ミス等によりインターネット上で個人データの閲覧が可能な状態となっていた
事例 4）個人データが記載・記録された書類・媒体等が盗まれた
事例 5）不正アクセス等により個人データを含む情報が第三者に盗まれた

※　当該個人データを第三者が閲覧しないうちに全てを回収した場合は「漏えい」に該当しない。
　また、事業者自身の意思による第三者提供は「漏えい」に該当しない。
※　金融機関等の関連情報の外部流出と「財産的被害発生のおそれ」との関係については、次のように考えられている。
　✧ 銀行口座情報だけが漏えい →財産的被害発生のおそれ 無
　✧ クレジットカード番号だけが漏えい →財産的被害発生のおそれ あり
　✧ クレジットカード番号の下 4 桁と有効期限の組合せが漏えい →財産的被害発生のおそれ 無
※　例えば、クレジットカードによる購入が可能なサイトのログイン番号とパスワードについて漏えい等が発生し、被害発生前にログイン番号とパスワードの再発行を含む被害防止が行われたとしても、基本的に報告が必要とされている。

滅　失 ➔

個人データの内容が失われること。

事例 1）個人情報データベース等を出力した帳票等を誤って廃棄した
事例 2）個人データが記載・記録された書類・媒体等を社内で紛失した

※　同じ内容のデータが他に保管されている場合は「滅失」に該当しない。事業者自身が合理的な理由により個人データを削除する場合も「滅失」に該当しない。
※　個人データが記載された帳票が適切に廃棄されていない場合、「漏えい」に該当する可能性がある。

毀　損 ➔

個人データの内容が意図しない形で変更されること、
あるいは、内容を保ちつつも利用不能な状態となること。

事例 1）個人データの内容が改ざんされた
事例 2）暗号化処理された個人データの復元キー喪失により、復元できなくなった
事例 3）ランサムウェア等により個人データが暗号化され、復元できなくなった

※　サイバー攻撃により個人データが利用できなくなると同時に個人データが盗まれた場合には、「漏えい」にも該当する。
※　事例 2・3 は、同じ内容のデータが他に保管されていれば「毀損」に該当しない。

■ 漏えい等が発覚した場合に講ずべき措置

漏えい等が発覚した場合に、ガイドラインでは次の５ 点について必要な措置を講ずることが求められています。

⑷ 事業者内部における報告及び被害の拡大防止
⑸ 事実関係の調査及び原因の究明
⑹ 影響範囲の特定
⑺ 再発防止策の検討及び実施
⑻ 個人情報保護委員会への報告及び本人への通知（義務は法令で規定する場合）

※　事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係や再発防止策等を速やかに公表することが望ましいとされています。

■ 行政への届出や本人への通知が義務付けられる漏えい等の範囲

情報の質的側面に着目したもの（性質として、個人の権利利益への侵害のおそれが大きいもの）として、要配慮個人情報を含むもの（1 号）や財産的被害につながるおそれのあるもの（2 号）が掲げられています。情報の量的側面に着目したものとして、1000 名分を超える場合（4 号）が掲げられています。その他に、行為態様の悪質性に着目したものとして、不正目的による漏えい（3 号）が掲げられています。

⑷ 要配慮個人情報が含まれる個人データの漏えい等、またはそのおそれ
事例 1）病院で患者の診療情報や調剤情報を含む個人データを記録した USB メモリーを紛失した場合
事例 2）従業員の健康診断等の結果を含む個人データが漏えいした場合
⑸ 不正利用により財産的被害を生ずるおそれのある個人データの漏えい等、またはそのおそれ
事例 1）EC サイトからクレジットカード番号を含む個人データが漏えいした場合
事例 2）送金や決済機能のある WEB サービスのログイン ID とパスワードの組み合わせを含む個人データが漏えいした場合
⑹ 不正目的をもって行われたおそれがある個人データの漏えい等、またはそのおそれ
事例 1）不正アクセスにより個人データが漏えいした場合（サイバー攻撃については、下記を参照）
事例 2）ランサムウェア等により個人データが暗号化され、復元できなくなった場合
事例 3）個人データが記載・記録された書類・媒体等が盗まれた場合
事例 4）従業員が顧客の個人データを不正に持ち出して第三者に提供した場合
※　従業員による個人データの持ち出し事案に関し、漏えいのおそれがある事例として、「個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合」が例示されています。
⑺ 1000 名分を超える個人データの漏えい等、またはそのおそれ
事例）システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、閲覧可能な個人が 1000 名を超える場合

～ いずれも、発生した場合だけでなく、「発生したおそれがある」場合も含まれます。「おそれ」の有無については個別の事案ごとに判断されますが、「その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合」は「おそれ」がある場合に該当するとされています。

《サイバー攻撃による漏えい等のおそれがある事例》

ガイドラインでは次の４ つが例示されています。

⑷ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合
⑸ 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合
⑹ マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ（C&C サーバ）が使用しているものとして知られている IP アドレス・FQDN（Fully Qualified DomainName の略。

サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの。）への通信が確認された場合

⑷ 不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合

■ 報告義務を負う者

当該個人データを取り扱う事業者が報告義務を負います。

個人データの取扱いを委託している場合、委託元と委託先の双方が当該個人データを取り扱っていることになるので、双方が報告義務を負います。ただし、委託により個人情報を取り扱っている者は、委託元に報告していれば、行政庁への届出や本人への通知義務は免れます。この場合、事態を知った後で速やかに（概ね 3～5 日以内）、委員会に報告すべき事項に関して、把握している限りの内容を全て委託元に通知する必要があります（施行規則 6 条の 4）。

■ 速報の取り扱い（施行規則 6 条の 3 第 1 項）

報告先 ➔

個人情報保護委員会

※ 個人情報保護法上の問題ではありませんが、生協の所管行政庁［都道府県 or 厚生労働省］にも報告が必要です。

報告の時期 ➔

生協のいずれかの部署の従業者が事態を知ってから概ね 3～5 日以内（「3～5 営業日」ではないので、土日祝日も含まれる）

報告する内容 ➔

⑷ 概要
　～ 発生日、発覚日、発生事案、発見者、分類（施行規則第 6 条の 2 各号のどれに該当するか）、委託元・委託先の有無、事実経過等を記載。

⑸ 当該個人データの項目
　～ 漏えい等が発生した情報項目（氏名、住所等）を、媒体（紙、電子媒体等）や種類（顧客情報、従業員情報等）とともに報告。

⑹ 当該個人データに係る人数

⑺ 原因
　～ 漏えい等がどこで発生したかを含めて記載。

⑻ 二次被害やそのおそれの有無・内容

⑼ 本人への対応の実施状況

⑽ 公表の実施状況

⑾ 再発防止のための措置
　～ 実施済みと今後実施予定に分けて報告。

⑿ その他参考となる情報

※ 報告の時点で把握している内容を報告します。

報告の方法 ➔

原則としてオンラインで報告する。
　～ 個人情報保護委員会 WEB サイトの報告フォーム（別紙）に入力。

■ 確報の取り扱い（施行規則 6 条の 3 第 2 項）

報告先 ➔

個人情報保護委員会

※ 個人情報保護法上の問題ではありませんが、生協の所管行政庁［都道府県 or 厚生労働省］にも報告が必要です。

報告の時期 ➔

生協のいずれかの部署の従業者が事態を知ってから 30 日以内（不正目的による漏えい等の場合は 60 日以内）

報告する内容 ➔

速報における報告内容と同様

※ 全てを報告する必要がありますが、合理的努力を尽くしても一部の事項が判明していない場合は、

その時点で把握している内容を報告し、判明次第報告を追完することが必要です。

報告の方法 ➔

速報と同様、原則としてオンラインで報告する。

■ 本人への通知（施行規則６ 条の５）

通知の時期 ➔

生協のいずれかの部署の従業員が事態を知ってから、「事態の状況に応じて速やかに」行う。

※　基本的に速やかに通知する必要がありますが、具体的にどの時点で通知するかは、「その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断」すべきとされています。加えて、「その時点で通知を行う必要があるとはいえないと考えられる事例」として、次の２ つが例示されています。

事例 1）漏えいした複数の個人データがインターネット上の掲示板にアップロードされており、生協から当該掲示板の管理者への削除要請など必要な初期対応が完了しておらず、本人に通知することで、かえって被害が拡大するおそれがある場合

事例 2）漏えい等のおそれはあるが、事案がほとんど判明しておらず、その時点で本人に通知しても本人が権利利益を守るための措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合

※　当初、漏えい等やそのおそれがあると思われたものの、その後の調査で実際にはそのようなことはなかったと判明した場合、本人への通知は不要とされています。

通知する内容 ➔

速報における報告内容のうち下記の事項に関し、「本人の権利利益を保護するために必要な範囲において」行う。

⑷ 概要
⑹ 当該個人データの項目
⑾ 原因
⑿ 二次被害やそのおそれの有無・内容
⒀ その他参考となる情報
～ 本人が権利利益を守るために取り得る措置など。

※　「本人の権利利益を保護するために必要な範囲」における通知の事例として、次の２ つが例示されています。

事例 1）不正アクセスによる漏えい事案で、原因に関し、個人情報保護委員会への報告内容から必要な内容のみを選択して本人に通知すること

事例 2）漏えい等が発生したデータ項目が本人ごとに異なる場合に、本人に関係する内容のみを通知すること。

通知の方法 ➔

ガイドライン上は、「事案の性質及び個人データの取扱状況に応じ、通知すべき内容が本人に認識される合理的かつ適切な方法」によるべきとされており、文書の郵送、電子メールの送信の２ つが例示されています。

通知の例外 ➔

本人への通知が困難である場合は、代替措置による対応が認められています。

＜本人への通知が困難な場合の例示＞

事例 1）保有する個人データの中に連絡先が含まれていない場合

事例 2）保有している連絡先が古く、現時点で連絡できない場合

＜代替措置の例示＞

事例 1）事案の公表

事例 2）本人からの問合せ窓口を用意してその連絡先を公表_