情報漏えい等の事態等対応手続

（目的）

第１条　本手続は、「個人情報の保護に関する法律」[1]及び「行政手続における特定の個人を識別するための番号の利用等に関する法律」に基づき、個人データ又は特定個人情報の漏えい、滅失又は毀損（それぞれ第２条第２項に定義する「漏えい」、「滅失」又は「毀損」をいう。以下併せて「漏えい等」という。）に関して報告対象事態（第２条に定める「報告対象事態」をいう。）が発生した場合における当社における対応についての手続について定める。なお、本規程の用語については、「個人情報取扱規程」及び「特定個人情報等取扱規程」の定めるところに従う。

（定義）[2]

第２条　この手続において「漏えい」とは、個人データ又は特定個人情報が外部に流出することをいう。

【個人データ／特定個人情報の漏えいに該当する事例】

事例 1）個人データ／特定個人情報が記載された書類を第三者に誤送付した場合

事例 2）個人データ／特定個人情報を含むメールを第三者に誤送信した場合

事例 3）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／特定個人情報の閲覧が可能な状態となっていた場合

事例 4）個人データ／特定個人情報が記載又は記録された書類・媒体等が盗難された場合

事例 5）不正アクセス等により第三者に個人データ／特定個人情報を含む情報が窃取された場合

なお、個人データ／特定個人情報を第三者に閲覧され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、個人情報取扱事業者が自らの意図に基づき個人データを第三者に提供する場合（原則として本人の同意が必要）は、漏えいに該当しない。

２　この手続において「滅失」とは、個人データ又は特定個人情報の内容が失われることをいう。

【個人データ／特定個人情報の滅失に該当する事例】

事例 1）個人情報データベース等／特定個人情報ファイルから出力された氏名等が記載された帳票等を誤って廃棄した場合（※1）

---

[1] 法 22 条の２【26 条】※令和２年改正法の「22 条」が令和３年改正法第一弾改正により「26 条」に変更されるため、条文番号を記載していない。

[2] 「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）」（以下「通則編ガイドライン」という。）3-5-1、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（以下「番号法ガイドライン」という。）「（別添２）特定個人情報の漏えい等に関する報告等（事業者編）」（以下「別添２」という。）㋑A・B・C

事例 2）個人データ／特定個人情報が記載又は記録された書類・媒体等を社内で紛失した場合（※2）

なお、上記の場合であっても、その内容と同じデータが他に保管されている場合は、滅失に該当しない。また、個人情報取扱事業者が合理的な理由により個人データ／特定個人情報を削除する場合は、滅失に該当しない。

（※１）当該帳票等が適切に廃棄されていない場合には、特定個人情報の漏えいに該当する場合がある。

（※２）社外に流出した場合には、特定個人情報の漏えいに該当する。

３　この手続において個人データ又は特定個人情報の「毀損」とは、個人データ又は特定個人情報の内容が意図しない形で変更されることや、内容を保ち通ｔも利用不能な状態となることをいう。

【個人データ／特定個人情報の毀損に該当する事例】

事例 1）個人データ／特定個人情報の内容が改ざんされた場合

事例 2）暗号化処理された個人データ／特定個人情報の復元キーを喪失したことにより復元できなくなった場合

事例 3）ランサムウェア等により個人データ／特定個人情報が暗号化され、復元できなくなった場合（※）

なお、上記の場合であっても、その内容と同じデータが他に保管されている場合は毀損に該当しない。

（※）同時に個人データ／特定個人情報が窃取された場合には、個人データ／特定個人情報の漏えいにも該当する。

（報告対象事態）[3]

第３条　当社は、次の第一号（１）から（４）まで及び第２号（１）から（３）までに掲げる事態（以下「報告対象事態」という。）を知ったときは、個人情報保護委員会に報告するものとする。ただし、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を講じているものはこの限りでない。

一　個人データ

（１）要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態

（例）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

（２）不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

[3] 個情法 22 条の２【第 26 条】１項、個情規則６条の２【７条】各号、番号法 29 条の４第１項、「行政手続における特定の個人を識別するための番号の利用等に関する法律第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則」（以下「特定個人情報漏えい報告等規則」という。）２条

（例）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

（３）不正の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が発生し、又は発生したおそれがある事態

（例）不正アクセスにより個人データが漏えいした場合

（例）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

（例）個人データが記載又は記録された書類・媒体等が盗難された場合

（例）従業者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

（４）個人データに係る本人の数が「1,000 人」を超える漏えい等が発生し、又は発生したおそれがある事態

（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、当該個人データに係る本人の数が 1,000 人を超える場合

二　特定個人情報

（１）次に掲げる事態

イ 不正の目的をもって行われたおそれがある特定個人情報の漏えい等が発生し、又は発生したおそれがある事態

（例）不正アクセスによって特定個人情報を漏えいした場合

（例）ランサムウェア等によって特定個人情報が暗号化され、復元できなくなった場合

（例）特定個人情報が記載又は記載された書類・媒体等が盗難された場合

ロ 不正の目的をもって、特定個人情報が利用され、又は利用されたおそれがある事態

（例）業務に関係なく、マイナンバーを利用し、住所等を検索・取得した場合

ハ 不正の目的をもって、特定個人情報が提供され、又は提供されたおそれがある事態

（例）従業者が特定個人情報を不正に持ち出して第三者に提供した場合

（２）特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態

（例）システムの設定ミス等によりインターネット上で特定個人情報の閲覧が可能な状態となっている場合

（３）次に掲げる特定個人情報に係る本人の数が「100 人」を超える事態

イ 漏えい等が発生し、又は発生したおそれがある特定個人情報

（例）第三者に誤送付・誤送信した特定個人情報に係る本人の数が 100 人を超える場合

ロ 番号法第９条の規定に反して利用され、又は利用されたおそれがある個人番号を含む特定個人情報

（例）個人番号利用事務と関係のない顧客管理のためのＩＤとして利用していたマイナンバーの数が 100 人を超える場合

ハ 番号法第 19 条の規定に反して提供され、又は提供された 100 人を超える特定個人情報の漏えい等が発生し、又は発生したおそれがある事態

（例）マイナンバー部分にマスキング処理することを失念して、特定個人情報を取り扱わない委託事業者等に提供した特定個人情報に係る本人の数が 100 人を超える場合。

（所管部署）

第４条　【総務部】を本手続の所管部署とし、以下の対応について、関係各部と連携して責任をもって行う。

（１）当社内部における報告・被害の拡大の防止[4]

報告対象事態を認識した者は総務部の事務取扱責任者に直ちに報告するものとする。漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講じなければならない。

（２）事実関係の調査、原因の究明[5]

事務取扱責任者は漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講じなければならない。

（３）影響範囲の特定[6]

事務取扱責任者は、上記（2）で把握した事実関係による影響範囲の特定のために必要な措置を講ずるものとする。

（４）再発防止策の検討及び実施[7]

事務取扱責任者は、上記（2）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講じるものとする。

（５）個人情報保護委員会への報告及び本人への通知[8]

２．事務取扱責任者である【総務部長】は本手続に定める対応を率先して行う。【総務部長】が不在の場合は、【総務副部長】が対応を代行する。

３．事務取扱責任者は、本手続について定期的（年１回程度）に見直しを行う。

（第一報）[9]

第５条　当社の従業者は、漏えい等の事案の発生を認識した場合には、【総務部】に報告を

---

[4] 通則編ガイドライン 3-5-2（１）、番号法ガイドライン別添 2(2)A
[5] 通則編ガイドライン 3-5-2（２）、番号法ガイドライン別添 2(2)B
[6] 通則編ガイドライン 3-5-2（３）、番号法ガイドライン別添 2(2)C
[7] 通則編ガイドライン 3-5-2（４）、番号法ガイドライン別添 (2)D
[8] 通則編ガイドライン 3-5-2（５）、番号法ガイドライン別添 (2)E
[9] 「個人データの漏えい等事案が発生した場合対応について」（平成 29 年個人情報保護委員会告示第１号、以下「漏えい等告示」）の「２（１）事業者内部における報告及び被害の拡大防止」

しなければならない。

【総務部】の連絡先：○○―○○○○―○○○○（内線○○、△△、××）

（被害の拡大の防止）[10]

第６条　事務取扱責任者は、前条の第一報があった場合、速やかに漏えい等の事案の防止その他の暫定措置を講ずるように関係部署に対して指示をする。

２．外部からの不正アクセスや不正プログラムの感染が疑われる場合には、当該端末等の LAN ケーブルを抜いてネットワークからの切り離しを行う等、適切な対応について、関係部署に対して指示をする。

（経営陣への報告）[11]

第７条　事務取扱責任者は、必要と認められる場合、直ちに、代表取締役及び関係担当取締役に対して報告を行う。

（事実関係の調査、原因の究明）[12]

第８条　事務取扱責任者は、関係部署と連携の上、以下の観点において事実関係の調査を行う。

（１）漏えい等があった個人情報を取扱う部署及び担当者の特定

（２）漏えい等のルートの解明

（３）漏えい等の有無の確認（漏えい等していた場合には、漏えい先の特定を含む。）

（４）漏えい等の対象となる本人、情報の項目及び人数の特定

２．事務取扱責任者は、原因の究明にあたっては、以下の観点により検討を行う。

（１）全社レベルの問題か・各部レベルの問題か

（２）社内規程等に不備がなかったか

（３）安全管理措置（組織的・人的・物理的・技術的）に不備はなかったか（特に、不正アクセスの場合は、技術的安全管理措置において情報システムシステムの脆弱性・不備はなかったか）

（４）組織全体の問題か・個人に起因する原因か

３．当社の情報システムに対する不正アクセスが認められる場合は、外部のフォレンジック専門業者に委託をして事実関係の調査及び原因の究明を行う。

４．事務取扱責任者は、必要に応じて、警察、弁護士等に対して相談を行う。

---

[10] 漏えい等告示の「２（１）事業者内部における報告及び被害の拡大防止」

[11] 漏えい等告示の「２（１）事業者内部における報告及び被害の拡大防止」

[12] 漏えい等告示の「２（２）事実関係の調査及び原因の究明」

（影響範囲の特定）[13]

第９条　事務取扱責任者は、前条で把握した事実関係に関して、漏えい等の対象となる情報の本人の数、漏えいした情報の内容、漏えいした原因等を踏まえ、影響範囲を特定する。

（再発防止策の検討及び実施）[14]

第 10 条　事務取扱責任者は、第７条で究明した原因及び前条で特定した影響範囲を踏まえ、再発防止策を検討し、速やかに実施する。

２．再発防止策は以下の観点に留意して策定するものとする。

（１）全社レベルの見直しが必要か、各部レベルの見直しで足りるか

（２）社内規程等の見直しが必要か

（３）安全管理措置（組織的・人的・物理的・技術的）の見直しが必要か

（４）運用の見直しやモニタリングで足りるか

（関係者の処分）

第 11 条　人事部長は、就業規則に基づき、関係者を懲戒処分等する。

２．事務取扱責任者は、必要に応じて、関係者について刑事告発を行う。

（個人情報保護委員会への報告）[15]

第 12 条　当社は、報告対象事態を知ったときは、速やかに（概ね３～５日以内）[16]、個人情報保護委員会に以下の事項のうち、その時点で把握している当該事態に関する事項を個人情報保護委員会所定の様式により報告しなければならない（速報）。報告期限の起算点となる「知った」時点については、当社のいずれかの部署が当該事態を知った時点を基準とする

①概要

②個人データ／特定個人情報の項目

③個人データ／特定個人情報に係る本人の数

④原因

⑤二次被害又はそのおそれの有無及びその内容

⑥本人への対応の実施状況

⑦公表の実施状況

⑧再発防止のための措置

⑨その他参考となる事項。

---

[13] 漏えい等告示の「２（３）影響範囲の特定」

[14] 漏えい等告示の「２（４）再発防止策の検討及び実施」

[15] 個情法 22 条の２【26 条】、個情法規則６条の３【８条】、番号法 29㉙条の４第１項、特定個人情報漏えい報告等規則３条

[16] 通則編ガイドライン 3-5-3-5、番号法ガイドライン別添２C

２．当社は、報告対象事態を知った日から 30 日以内（第２条第１号（３）又は第２号（１）イからロまでの事態を知った場合には 60 日以内）に、第１項に掲げる当該事態に関する事項を個人情報保護委員会所定の様式により記載の事項を個人情報保護委員会に報告しなければならない（確報）。

（本人への通知）[17]

第 13 条　個人情報取扱事業者は、報告対象事態（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を講じている場合を除く。）を知ったときは、当該事態の状況に応じて速やかに、第３項に規定する事項を本人に通知するものとする。

２．「当該事態の状況に応じて速やかに」とは、速やかに通知を行うことを求めるものであるが、具体的に通知を行う時点は、個別の事案において、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るものとする。

【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（※）】

＊ インターネット上の匿名掲示板等に漏えいした複数の特定個人情報がアップロードされており、個人番号利用事務等実施者において当該掲示板等の管理者に削除を求める等、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

＊ 漏えい等のおそれが生じたものの、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たとしても、本人がその権利利益を保護す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

（※）「当該事態の状況に応じて速やかに」本人への通知を行うべきことには変わりない。

３．本人への通知事項は、当該本人の権利利益を保護するために必要な範囲において以下の事項を通知するものとする。

①　概要
②　漏えい等が発生し、又は発生したおそれがある個人データの項目
③　原因
④　二次被害又はそのおそれの有無及びその内容
⑤　その他参考となる事項

４．第１項にかかわらず、、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとる場合には本人への通知を要しない。[18]

【本人への通知が困難な場合に該当する事例】

---

[17] 個情法 22 条の２【26 条】、個情法規則６条の３【８条】、番号法 29 条の４第２項、特定個人情報漏えい報告等規則５条

[18] 個情法 22 条の２【第 26 条】第２項ただし書、番号法㉙条の４第２項ただし書

事例 1）保有する個人データの中に本人の連絡先が含まれていない場合
事例 2）連絡先が古いために通知を行う時点で本人へ連絡できない場合
【代替措置に該当する事例】
事例 1）事案の公表
事例 2）問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにすること
（※）代替措置として事案の公表を行わない場合であっても、当該事態の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、公表を行うことが望ましい。
（※）公表すべき内容は、個別の事案ごとに判断されるが、本人へ通知すべき内容を基本とする。

（影響を受ける可能性のある本人への賠償）
第 14 条　事務取扱責任者は、漏えい等の事案が発生した場合、漏えい等の対象となった情報の内容、漏えい等の態様等の事実関係及び究明した原因、他の同種事案における賠償額等を考慮して、影響を受ける可能性のある本人への賠償額（金銭以外の賠償を含む。）及び賠償方法を決定する。

（事実関係及び再発防止策の公表）[19]
第 15 条　事務取扱責任者は、漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生回避等の観点から、事実関係及び再発防止策等について、速やかに公表するものとする。
２．前項にかかわらず、本人の権利利益が侵害されていないと認められる場合（以下の場合をも含むがこれらの場合に限られない）には、事実関係及び再発防止策等についての公表を省略することができる。なお、サイバー攻撃による場合等で、公表することでかえって被害の拡大につながる可能性があると考えられる場合には、専門機関等に相談するものとする。
（１）紛失したデータを第三者に見られることなく速やかに回収した場合
（２）高度な暗号化等の秘匿化が施されていて紛失したデータだけでは本人の権利利益が侵害されていないと認められる場合

（改廃）
第 16 条　本規程の改廃は、取締役会の決定により行うものとする。

附則
本規程は、令和〇年〇月〇日より施行する。

[19] 通則編ガイドライン 3-5-4-2、番号法ガイドライン別添 2 4A