１９．漏えい等が発生した場合の対応（ガイドライン第２２条）

１９－１．本人に通知

［ガイドライン］

第22条　電気通信事業者は、個人情報の漏えいが発生した場合は、速やかに、当該漏えいに係る事実関係を本人に通知するものとする。ただし、当該個人情報の漏えいがノートブック型パーソナルコンピュータ等の紛失又は盗難により発生したものであって、かつ、本人に対して二次被害が生じないよう適切な技術的保護措置が講じられているときは、この限りでない。

（第22条第1項の解説）

(1) 第１項は、個人情報の漏えいが発生した場合は、その個人情報の本人が適切に対応できるようにするため、電気通信事業者は事実関係を本人に速やかに通知することを規定するものである。なお、利用者が住所、電話番号、メールアドレスの変更等をし、これを電気通信事業者に通知していないときなど本人の連絡先が不明である場合には、通知できなくてもやむを得ないと考えるが、こうした場合はできるだけ本人が個人情報の漏えいの事実を把握できるように第２項に従って公表を行うことが求められる。

なお、個人情報の「滅失又はき損」は、個人情報の本人の権利利益には影響がない場合もあるので、本ガイドラインでは、個人情報の滅失又はき損が発生した場合に一律に本人への通知を要するものとはしていない（第2項及び第3項との違いに留意）が、個人情報の本人の権利利益に影響が生じるような場合には本人に通知することとすべきであろう。

(2) 第１項ただし書は、漏えいが発生した個人情報に対して本人への二次被害が生じないよう適切な技術的保護措置が講じられている場合には、本人へ通知しないことができるとしたものである。なお、企業によっては、広く情報開示を行うことを表明しているケースも考えられることから、本人への通知を行うか否かについては、電気通信事業者の判断によるものである。

「ノートブック型パーソナルコンピュータ等」とは、個人情報が記録可能な機器であるノートブック型のパーソナルコンピュータのほか、携帯電話端末、PDA等の通信端末機器、USBなどの外部記録媒体等の一般に持ち出して利用される機器を念頭に置いたものである。

「適切な技術的保護措置」の具体的な措置内容については、次の①～③のいずれも満たす場合である。

① 高度な暗号化措置が講じられていること

電子政府推奨暗号リスト又はISO/IEC18033に掲げられている暗号アルゴリズムによって、記録媒体内の個人情報の保存先として利用可能な全領域が自動的に暗号化されること。

② 暗号化された情報及び復号鍵の管理が適切にされていること

次の（ｉ）又は（ⅱ）の方法によって暗号化された情報及びその暗号化された情報を復号させる復号鍵の管理が適切にされていること。ただし、使用する暗号化措置は、（ｉ）の方法においては暗号化された情報から分離された復号鍵の、（ⅱ）の方法においては遠隔操作により削除された復号鍵の権限者以外による不正な複製及び再生成ができないこと。

（ｉ）次のア又はイの方法によって暗号化された情報と復号鍵が分離されていること

ア 復号鍵のすべてが暗号化された情報と分離され、紛失した暗号化された情報の復号鍵が権限者の管理下に置かれるように構成されていること。

イ 公知の方式を用いかつ分散された情報の一部からの全体の復元が不可能であることが立証された秘密分散技術によって復号鍵が分散保存され、当該復号鍵の構成部分のうち、紛失した暗号化された情報と分離されない構成部分では復号ができずかつ紛失した暗号化された情報と分離されているすべての構成部分は権限者の管理下に置かれるように構成されていること。

（ⅱ）遠隔操作により記憶媒体内の復号鍵又は暗号化された情報（あるいはその両方）を削除できかつ記憶媒体内の復号鍵又は情報を削除するまでの間に、復号鍵の複製、情報の閲覧、複写がされていないことを権限者側で確認できること。

③ 個人情報の漏えい等に際し、①及び②の技術的保護措置が有効に実施されていること。

電気通信事業者の保有する個人情報が当該事業者の管理下を離れた場合には個人情報の漏えいと解され得るところ、具体的には次のような事例が個人情報の漏えいに該当し得るものである。

- 従業者又は委託先従業者による個人情報の不正な持出し
- 従業者又は委託先従業者の不注意による個人情報を含む書類等の誤送付
- 個人情報を含む書類、コンピュータ、記録媒体等の盗難・紛失
- システムの設定ミス又はシステムの安全管理措置が不十分であったことによりインターネット上で個人情報の閲覧が可能となっている
- 電子メールの誤配信（ＢＣＣ欄に記載すべきメールアドレスをＴＯ欄やＣＣ欄に記載して送信してしまった場合やメールアドレスを別人のものと取り違えをして送信した場合など）
- 本人の同意なき個人情報の第三者への提供（ガイドライン第１５条第１項各号に該当する場合を除く。）等

なお、漏えい事故の発生の際、現場において適切な対処が行われないと、被害の拡大や企業への信頼に甚大な影響を及ぼすおそれがある。

このような事態を防ぐためには、事前に内部の危機管理体制を定め、漏えい等が発生した場合に行うべき措置等に関するフロー等（注）を用意しておくことが望ましい。

（注）電気通信個人情報保護推進センターにおいては、対象事業者への情報提供の一環として、「漏えい対処フローチャート」及び「個人情報漏えい対応の留意点」を作成し、対象事業者に活用いただいているところです。

個人情報の漏えいが発生した場合、電気通信事業者は、次の項目を含め事実関係を速やかに確認した上で、本人に通知するものとする。

- 当該漏えいに係る被害者及び規模（人数）
- 当該漏えいに係る個人情報の項目（氏名、住所、電話番号、クレジットカード番号等）
- 当該漏えいの発生場所
- 当該漏えいの発生状況（発覚や確認の経緯も含む。）
- 当該漏えいの発生原因

これらの情報のほか、可能な限り次の情報についても、本人に対して丁寧に説明し、利用者の不安を取り除くことや必要な注意喚起を行うことに努めるべきである。

- 当該漏えいに伴う二次被害が発生する可能性（例えば、クレジットカード情報を保存していたノートパソコンを紛失した場合に、パスワードの設定等の安全管理措置を講じておらず、第三者にクレジットカードを不正利用されるおそれがあるため、速やかにクレジットカードの利用停止措置をとる必要があると考えられるときにはその旨）
- 二次被害を回避するために講ずる措置（電話番号やパスワードの変更を無料で受け付けるなど）
- 再発防止策　等

〇（好ましい事例）

事例１９－１　個人情報の漏えいが発生した場合に、速やかに事実関係を確認し、本人に当該事実関係を連絡し、架空請求や振り込め詐欺などの２次被害に遭わないよう注意喚起をするとともに、被害者から了解を得る。

×（好ましくない事例）

事例１９－２　個人情報の漏えいが発生した場合に、本人や国民からのクレームを恐れるあまり、事実関係を本人に通知するという意思決定に時間がかかってしまい、個人情報の漏えいが発生してからかなりの時間が経過してから実際に本人に事実関係を通知する。

事例１９－３　個人情報の漏えいが発生した場合に、本人に事実関係を電子メールや郵便で通知したが、そのうち一部が宛先不明で戻ってきたにもかかわらず、そのまま放置する。

≪参考事例≫
配達記録がある郵便で送付した通信サービスの強制解約予告通知が紛失したという事案において、電気通信事業者と郵便局が協力して調査し、郵便局において紛失したことを確認し、電気通信事業者は総務省への事故報告等を行うとともに、郵便局に抗議を行い、また、郵便局は利用者に謝罪を行ったという事例があった。

なお、漏えいが発生した個人情報に対して本人への二次被害が生じないよう適切な技術的保護措置が講じられている場合には、本人へ通知しないことができるとされているが、適切な技術的保護措置が講じられている場合とは、①高度な暗号化措置が講じられていること、②暗号化された情報及び復号鍵の管理が適切にされていること、③個人情報漏えいに際し、①及び②の技術的保護措置が有効に実施されていることのいずれも満たす場合である。

ここでいう「適切な技術的保護措置」については、参考資料２に詳しく解説してあるので参照されたい。

適切な技術的保護措置が講じられている場合であっても、電気通信事業者によっては、広く情報開示を行うことを表明していることも考えられることから、電気通信事業者の判断により本人への通知を行うことを妨げるものではない。

＜適切な技術的保護措置が講じられている場合において、本人への通知を省略してもよい例＞

- 個人情報を保存していたノートパソコンを紛失したが、高度な暗号化措置（電子政府推奨暗号リスト又はＩＳＯ/ＩＥＣ１８０３３に掲げられている暗号アルゴリズムによる暗号化措置）、暗号化された情報及び復号鍵の適切な管理がされていたので、直ちに本人へ二次被害が生じるものではないと考えられるため、本人への通知を行わないこととした。
- 保有しているすべてのノートパソコンに電子政府推奨暗号リストに掲げられている暗号アルゴリズムによりハードディスクの利用可能な全領域が自動的に暗号化できるシステムを導入し、また、復号鍵はパスワード付のＵＳＢメモリに別管理をしていたので、個人情報を保存していたノートパソコンの紛失が発生したが、本人への二次被害が生じるものとは考えられないので、本人への通知を行わないこととした。

１９－２．公表

［ガイドライン第22条］

第2項　電気通信事業者は、個人情報の漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り、当該漏えい等に係る事実関係その他の二次被害の防止、類似事案の発生回避等に有用な情報を公表するものとする。ただし、当該個人情報の漏えい等がノートブック型パーソナルコンピュータ等の紛失、盗難、破損等により発生したものであって、かつ、本人に対して二次被害が生じないよう適切な技術的保護措置が講じられているときは、この限りではない。

（第22条第2項の解説）

(3)　第2項は、個人情報の漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することを規定するものである。なお、「漏えい等」とは、「漏えい、滅失又はき損」を指す（第１１条参照。第3項も同じ。）。「可能な限り」とは、セキュリティーの観点から公表するとかえって二次被害の拡大や類似事案の増大につながるようなものは公表することは要しないが、それ以外の事実関係等については二次被害の防止、類似事案の発生回避等に有用な情報をできるだけ公表すべきとの趣旨である。また、事実関係のほかに公表すべき「二次被害の防止、類似事案の発生回避等に有用な情報」には、再発防止策などが含まれる。

同項ただし書は、(2)と同様の考え方によるものである。

「二次被害」とは、漏えいした個人情報が第三者に悪用されることにより本人に発生する被害などをさすものと考えられ、具体的には

- 勧誘や嫌がらせの電話がかかってきたり、いわゆる迷惑メールが送信されたり、ストーカー行為が行われる
- いわゆる架空請求の葉書等が送られてきたり、振込め詐欺電話がかかってきたりして実際に金銭的な被害が発生する
- 当該情報が、Ｗｅｂ上の掲示板、Ｐ２Ｐソフトウェアなどを介して広く流通し本人のプライバシーが侵害される

などの事例が考えられる。個人情報の漏えいが発生したときは、その個人情報の本人が適切に対応できるようにするため、事実関係を速やかに本人に通知することとされているが（前項参照）、利用者が住所、電話番号、メールアドレスの変更等をし、これを電気通信事業者に通知していないときや、通知の対象者が多く対象者全員への通知が終わるまでに二次被害が発生するおそれがあるような場合には、事実関係の公表を通じて、本人が適切に対応できるようにし又は漏えいした個人情報を持っている者に対する警告をすることで、二次被害の防止に資することとなると考えられることから、可能な限り事実関係を公表す

るものとする。また、事実関係の公表により、他の電気通信事業者に対して注意喚起をすることとなり、類似事案の発生を回避する効果も期待できる。

一方で、セキュリティーの観点から、公表するとかえって二次被害の増大や類似事案の増大につながるようなものは公表することを要しないこととしているが、これは、例えば個人情報漏えいの原因やその再発防止策を公開してしまうと、セキュリティーホールを狙った不正アクセス等の増加を助長する可能性も十分考えられるためである。したがって、事実関係その他の二次被害の防止、類似事案の発生回避等に有用な情報を公表する場合には、公表する情報の範囲についてよく検討するべきである。

また、事実関係を公表する際は、当該電気通信事業者において講じてきた安全管理措置や当該電気通信事業者における個人情報保護に対する取組姿勢についても併せて公表することとし、利用者の不安を取り除くよう努めることも重要である。

○（好ましい事例）

事例１９－４　外部からの指摘により、自社の個人情報がインターネット上で閲覧可能になっていることが判明したときに、速やかにシステムの運用を停止し、個人情報の漏えいの事実は公表するが、セキュリティーの観点から原因及び再発防止策の詳細は公表しない。

事例１９－５　お客様から個人情報の漏えいの疑いの問い合わせを受け、事実関係を調査した結果、自社の個人情報が漏えいしたものと判断するに至った場合、速やかにその事実関係を公表する。さらに原因が判明し、再発防止策の目処が付いた段階で、改めてその旨を公表する。

事例１９－６　部外者を名乗る者から「貴社の個人情報を入手した」という連絡があり、恐喝めいたことを言われたため、警察に相談したところ、事実関係の公表は控えるよう要請されたため、当面は事実関係を公表しない。

×（好ましくない事例）

事例１９－７　社外からの通報で個人情報の漏えいの可能性を認識した際に、十分な事実関係の確認をせずに、公表してしまい、マスコミや利用者から事実関係に関する質問攻めに遭い、回答内容に一貫性を欠く。

事例１９－８　社外からの通報で個人情報の漏えいの可能性を認識し、調査の結果、個人

情報の漏えいの事実を確認したにもかかわらず、当該事実を関係者の間で隠蔽する。

なお、漏えい等が発生した個人情報に対して本人への二次被害が生じないよう適切な技術的保護措置が講じられている場合には、公表しないことができるとされているが、適切な技術的保護措置が講じられている場合とは、①高度な暗号化措置が講じられていること、②暗号化された情報及び復号鍵の管理が適切にされていること、③個人情報漏えい等に際し、①及び②の技術的保護措置が有効に実施されていることのいずれも満たす場合である。

ここでいう「適切な技術的保護措置」については、参考資料２に詳しく解説してあるので参照されたい。

適切な技術的保護措置が講じられている場合であっても、電気通信事業者によっては、広く情報開示を行うことを表明していることも考えられることから、電気通信事業者の判断により公表することを妨げるものではない。

また、類似事案の発生回避の観点からは、事業者それぞれの個別の公表ではなく、類似事案発生のおそれがある事実について総務省による発表等の手段により、個別の公表に代替することが可能である。

＜適切な技術的保護措置が講じられている場合において、個別の公表を省略してもよい例＞

- 個人情報を保存していたノートパソコンを紛失したが、高度な暗号化措置（電子政府推奨暗号リスト又はＩＳＯ／ＩＥＣ１８０３３に掲げられている暗号アルゴリズムによる暗号化措置）、暗号化された情報及び復号鍵の適切な管理がされていたので、直ちに本人へ二次被害が生じるものではないと考えられるため、公表を行わないこととした。

１９－３．報告

[ガイドライン　第22条]
第3項　電気通信事業者は、個人情報の漏えい等が発生した場合は、当該漏えい等に係る事実関係を総務省に直ちに報告するものとする。ただし、当該個人情報の漏えい等がノートブック型パーソナルコンピュータ等の紛失、盗難、破損等により発生したものであって、かつ、本人に対して二次被害が生じないよう適切な技術的保護措置が講じられているときは、四半期内に発生した個人情報の漏えい等の事実関係を当該四半期経過後遅滞なく報告することを持って代えることができる。

（第22条第3項の解説）
(4)　第3項は、個人情報の漏えい等が発生した場合は、事実関係を総務省に直ちに報告することを規定するものである。
　同項ただし書は、漏えい等の発生した個人情報に本人への二次被害が生じないよう適切な技術的保護措置が講じられていた場合には、四半期内に発生した個人情報の漏えい等の事実関係を毎四半期経過後一定期間（概ね一月）内に、一括して総務省に報告することができるようにしたものである
　この場合における四半期とは、4月から6月まで、7月から9月まで、10月から12月まで及び1月から3月までのそれぞれの期間である。
　なお、報告に当たっては、個人情報の漏えい等の発生に際し、本人への二次被害が生じないようにするために講じられていた技術的保護措置の内容及びその措置が確実に実行されていたとする理由を含める必要がある。

電気通信事業者は、その保有に係る個人情報（電気通信事業者の社員情報を含む。）の漏えい等が発生した場合（個人情報の取扱いを委託している場合において当該委託先から漏えいした場合を含む。）は、口頭又は文書により、直ちに総務省に事実関係を連絡することが必要である。その後、利用者対応の状況、新たに判明した事実関係及び再発防止策を加えて、当該漏えい等について報告書(注)にまとめて提出することとすべきである。

（注）総務省においては特に報告書の様式を定めていないとのことであるが、電気通信事業法施行規則様式50の2に準ずる様式で報告されるのが通例とのことである（ただし、記載事項は様式50の2とは若干異なる。）。様式例を別紙に示す。

なお、漏えい等の発生した個人情報に本人への二次被害が発生しないよう適切な技術的保護措置が講じられていた場合には、個人情報の漏えい等の事実関係を四半期毎に一括して報告することも可能であるとされているが、適切な技術的保護措置が講じられている場合とは、①高度な暗号化措置が講じられている

こと、②暗号化された情報及び復号鍵の管理が適切にされていること、③個人情報漏えい等に際し、①及び②の技術的保護措置が有効に実施されていることのいずれも満たす場合である。

ここでいう「適切な技術的保護措置」については、参考資料２に詳しく解説してあるので参照されたい。

一括して報告する時期は、第一四半期（４月から６月）であれば７月中、第二四半期（７月から９月）であれば１０月中ということである。

また、一括して報告する場合においては、講じられていた技術的保護措置の内容及びその措置が確実に実行されていた根拠を記載する必要がある。

＜適切な技術的保護措置が講じられている場合において、四半期分を一括して報告してもよい例＞

- 第一四半期に複数の個人情報の漏えい事故を発生させたが、本人への二次被害が発生しないよう適切な技術的保護措置を講じていたので、技術的保護措置の内容とその措置が確実に実行されていた根拠を含め、７月下旬に一括して総務省へ報告した。

ただし、社員情報については、雇用管理に関する個人情報でもあり、個人情報保護法第３６条（主務大臣）の規定により、厚生労働大臣及び事業の所管大臣（電気通信事業の場合は総務大臣）が主務大臣となっている。したがって、社員情報は、厚生労働省の「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（厚生労働省告示第２５９号平成１６年７月１日）の対象にもなっていることに留意する必要がある。

なお、電気通信業務に関して通信の秘密の漏えいが生じたときは、電気通信事業法第２８条及び電気通信事業法施行規則第５７条の規定に基づき、速やかにその発生日時及び場所、概要、理由又は原因、措置模様などを総務大臣に報告するとともに、漏えいを知った日から３０日以内に総務大臣あてに同規則様式５０の２の報告書を提出しなければならない。

１９－４．電気通信個人情報保護推進センターへの連絡

対象事業者は、個人情報の漏えい等が発生した場合、当該事実関係を電気通信個人情報保護推進センターへ連絡することも必要である。当協会の対象事業者である電気通信事業者は、苦情の申出先として、当センターを本人の知り得る状態に置くこととされていることから、当センターへも苦情や問い合わせが寄せられることが想定され、その対応のため、当センターにおいても事実関係を把握しておく必要があるからである。

なお、漏えい等の発生した個人情報に本人への二次被害が発生しないよう適切な技術的保護措置が講じられていて、総務省へ個人情報の漏えい等の事実関係を四半期毎に一括して報告する場合には、当センターへも一括して連絡することが可能である。

＜連絡する事実関係の項目＞

① 事故の種類
② 発生日時（又は発見日時）
③ 発生場所
④ 発生原因
⑤ 被害者及び規模（人数）
⑥ 漏えいに係る個人情報の項目
⑦ 被害者への連絡状況
⑧ 総務省報告日
⑨ 公表の有無
⑩ その他

- 媒体へのセキュリティーの状況
- 応急対応措置
- 顧客対応窓口の設置状況
- 警察への届出の有無
- その他、苦情対応上有意義な情報

〇（好ましい事例）

事例１９－９　個人情報（電気通信事業者の社員情報を含む。）の漏えいが発生した場合に、速やかに事実関係を確認し、本人へ通知するとともに、総務省へ第一報する。その後、利用者対応の状況、新たに判明した事実関係及び再発防止策を含めて当該漏えいについて報告書にまとめて総務省に提出する。

ただし、社員情報は、厚生労働省の「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」の対象にもなっていることから、社員情報の漏えいが発生した場合には、総務省に報告するほか厚生労働省から報告を求め

られることがあることに留意。

×（好ましくない事例）

事例１９－１０　個人情報の漏えいが発生した場合に、速やかに事実関係を確認し、本人へ通知するとともに、事実関係の公表をしたが、総務省への報告を怠ってしまった。