電気通信事業における個人情報保護に関するガイドライン解説の一部改正案新旧対照表　（傍線部分は改正部分）

| 改正案 | 現行 |
| --- | --- |
| **電気通信事業における個人情報保護に関するガイドライン（平成 16 年総務省告示第 695 号。最終改正平成 22 年総務省告示〇〇号）の解説** | **電気通信事業における個人情報保護に関するガイドライン(平成 16 年総務省告示第 695 号。最終改正平成 21 年総務省告示 543 号）の解説** |
| **（利用目的の特定）**<br>**第５条　電気通信事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定するものとする。**<br>**２　電気通信事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行わないものとする。**<br>**３　前２項の規定により特定する利用目的は、電気通信サービスを提供するため必要な範囲を超えないものとする。** | **（利用目的の特定）**<br>**第５条　電気通信事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定するものとする。**<br>**２　電気通信事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行わないものとする。**<br>**３　前２項の規定により特定する利用目的は、電気通信サービスを提供するため必要な範囲を超えないものとする。** |
| （解説）<br>(1) 本条は、個人情報の適正な取扱いを実現するための前提として、電気通信事業者に対して、その利用目的をできる限り特定させるとともに、その変更も一定の合理的な範囲に留めるものとすること、及び、利用目的が電気通信サービスを提供するため必要な範囲を超えないものとすることを規定するものである。なお、本条や次条等の個人情報の「利用」とは、第１５条の第三者への提供を含む概念である。<br>(2) 「その利用の目的を…できる限り特定」するとは、個人情報がどのような目的で利用されるかをできるだけ具体的に明確にするという趣旨である。したがって、単に「サービスの提供のため」や「業務の遂行のため」といった抽象的な目的では足りず、例えば、「加入者の本人確認、料金の請求、料金・サービスの変更及びサービスの休廃止の通知のため、加入者の氏名、住所、電話番号を利用します。」のように具体的に特定すべきである。<br>なお、個人情報に対して、特定の個人を識別できないようにする加工（いわゆる匿名化）を行うことは、個人情報の利用に当たらず、利用目的として特定 | （解説）<br>(1) 本条は、個人情報の適正な取扱いを実現するための前提として、電気通信事業者に対して、その利用目的をできる限り特定させるとともに、その変更も一定の合理的な範囲に留めるものとすること、及び、利用目的が電気通信サービスを提供するため必要な範囲を超えないものとすることを規定するものである。なお、本条や次条等の個人情報の「利用」とは、第１５条の第三者への提供を含む概念である。<br>(2) 「その利用の目的を…できる限り特定」するとは、個人情報がどのような目的で利用されるかをできるだけ具体的に明確にするという趣旨である。したがって、単に「サービスの提供のため」や「業務の遂行のため」といった抽象的な目的では足りず、例えば、「加入者の本人確認、料金の請求、料金・サービスの変更及びサービスの休廃止の通知のため、加入者の氏名、住所、電話番号を利用します。」のように具体的に特定すべきである。 |

| | |
|---|---|
| する必要はない。<br>(3) 第２項は、いったん特定された利用目的が無限定に変更されることとなれば、利用目的を特定させる実質的意味は失われることから、利用目的の変更は認めるものの、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲に留めるべきであることとするものである。変更の許容範囲を超えた利用目的で個人情報を利用する場合には、本人の同意を得るか、新たに利用目的を定めて再度個人情報を取得する必要がある。<br>「相当の関連性を有する」とは、いったん特定された利用目的からみて、想定されることが困難でない程度の関連性を有することをいう。また、「合理的に認められる」とは、社会通念上妥当であると客観的に認識されるとの趣旨である。<br>(4) 第３項は、前条第１項の個人情報の取得は電気通信サービスを提供するため必要な場合に限るとの規定を受けて、第１項及び第２項の規定により特定する利用目的も電気通信サービスを提供するため必要な範囲を超えないものとすることを確認的に規定するものである。 | (3) 第２項は、いったん特定された利用目的が無限定に変更されることとなれば、利用目的を特定させる実質的意味は失われることから、利用目的の変更は認めるものの、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲に留めるべきであることとするものである。変更の許容範囲を超えた利用目的で個人情報を利用する場合には、本人の同意を得るか、新たに利用目的を定めて再度個人情報を取得する必要がある。<br>「相当の関連性を有する」とは、いったん特定された利用目的からみて、想定されることが困難でない程度の関連性を有することをいう。また、「合理的に認められる」とは、社会通念上妥当であると客観的に認識されるとの趣旨である。<br>(4) 第３項は、前条第１項の個人情報の取得は電気通信サービスを提供するため必要な場合に限るとの規定を受けて、第１項及び第２項の規定により特定する利用目的も電気通信サービスを提供するため必要な範囲を超えないものとすることを確認的に規定するものである。 |

| 改正案 | 現行 |
| --- | --- |
| **（安全管理措置）**<br>**第１１条　電気通信事業者は、個人情報へのアクセスの管理、個人情報の持出し手段の制限、外部からの不正なアクセスの防止のための措置その他の個人情報の漏えい、滅失又はき損（以下「漏えい等」という。）の防止その他の個人情報の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講ずるものとする。**<br>**２　電気通信事業者は、安全管理措置を講ずるに当たっては、情報通信ネットワーク安全・信頼性基準（昭和６２年郵政省告示第７３号）等の基準を活用するものとする。** | **（安全管理措置）**<br>**第１１条　電気通信事業者は、個人情報へのアクセスの管理、個人情報の持出し手段の制限、外部からの不正なアクセスの防止のための措置その他の個人情報の漏えい、滅失又はき損（以下「漏えい等」という。）の防止その他の個人情報の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講ずるものとする。**<br>**２　電気通信事業者は、安全管理措置を講ずるに当たっては、情報通信ネットワーク安全・信頼性基準（昭和６２年郵政省告示第７３号）等の基準を活用するものとする。** |
| （解説）<br>(1) 本条は、電気通信事業者が、個人情報を取り扱うに当たり、個人情報を安全に管理するための措置を講ずるものとすることを規定したものである。<br>安全管理措置は、技術的保護措置及び組織的保護措置に大きく分類され、その双方を適切に実施することが必要である。<br>その際には、本人の個人情報が漏えい等した場合に本人に与える影響等を考慮し、通信の秘密に該当するもの等、より重大な影響を及ぼす可能性がある個人情報については、より厳格に取り扱うこととする等の措置をとることが適当である。<br>なお、例えば、不特定多数者が書店で随時に購入可能な名簿で、電気通信事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、電気通信事業者の安全管理措置の義務違反にはならない。<br>(2) 技術的保護措置とは、<br>① 個人情報へのアクセスの管理（アクセス権限者の限定（異動・退職した社 | （解説）<br>(1) 本条は、電気通信事業者が、個人情報を取り扱うに当たり、個人情報を安全に管理するための措置を講ずるものとすることを規定したものである。<br>安全管理措置は、技術的保護措置及び組織的保護措置に大きく分類され、その双方を適切に実施することが必要である。<br>その際には、本人の個人情報が漏えい等した場合に本人に与える影響等を考慮し、通信の秘密に該当するもの等、より重大な影響を及ぼす可能性がある個人情報については、より厳格に取り扱うこととする等の措置をとることが適当である。<br>なお、例えば、不特定多数者が書店で随時に購入可能な名簿で、電気通信事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、電気通信事業者の安全管理措置の義務違反にはならない。<br>(2) 技術的保護措置とは、<br>① 個人情報へのアクセスの管理（アクセス権限者の限定（異動・退職した社 |

| | |
|---|---|
| 員のアカウントを直ちに無効にする等の措置を含む。）、アクセス状況の監視体制（アクセスログの長期保存等）、パスワードの定期的変更、入退室管理等）<br>② 個人情報の持出し手段の制限（みだりに外部記録媒体へ記録することの禁止、社内と社外との間の電子メールの監視を社内規則等に規定した上で行うこと等）<br>③ 外部からの不正アクセスの防止のための措置（ファイアウォールの設置等）などの内部からの情報漏えい及び外部からの不正アクセスの双方を防止するための物理的・技術的措置を指すが、上記①～③のほか、情報通信ネットワーク安全・信頼性基準その他の国内・国際の公表されている情報セキュリティーに関する基準を活用して、各電気通信事業者が個人情報の取扱状況に応じた適切な内部規程・マニュアルを策定し、実施することが必要である。<br>なお、事業用電気通信設備（電気通信回線設備及び基礎的電気通信役務を提供する電気通信事業の用に供する電気通信設備）に関する技術的保護措置については、事業用電気通信設備を設置する電気通信事業者に対し、事業用電気通信設備規則（昭和６０年郵政省令第３０号）に定める技術基準の適合維持義務が課されている（電気通信事業法第４１条）ことにも留意する必要がある。<br>(3) 組織的保護措置とは、<br>① 安全管理に関する従業者・委託先の責任と権限を明確に定めること<br>② 安全管理に関する内部規程・マニュアルを定め、それらを従業者に遵守させるとともに、その遵守の状況について適切な監査を行うこと<br>③ 従業者・委託先と秘密保持契約を締結すること等により安全管理について従業者・委託先を適切に監督すること<br>④ 安全管理について従業者に対し必要な教育研修を行うこと<br>などの人的・組織的な措置を指すが、これらの事項については、次条及び第１３条に詳細な規定がおかれているので、それらの規定の解説を参照されたい。<br>(4) 個人情報をパーソナルコンピュータ、外部記録媒体等で社外に持ち出す場合には、パーソナルコンピュータ等が紛失、盗難することによって個人情報が漏えいするリスクが問題になる。そのため、リスクに備え、持ち出した個人情報の安全性が確保されるよう措置を講じる必要がある。 | 員のアカウントを直ちに無効にする等の措置を含む。）、アクセス状況の監視体制（アクセスログの長期保存等）、パスワードの定期的変更、入退室管理等）<br>② 個人情報の持出し手段の制限（みだりに外部記録媒体へ記録することの禁止、社内と社外との間の電子メールの監視を社内規則等に規定した上で行うこと等）<br>③ 外部からの不正アクセスの防止のための措置（ファイアウォールの設置等）などの内部からの情報漏えい及び外部からの不正アクセスの双方を防止するための物理的・技術的措置を指すが、上記①～③のほか、情報通信ネットワーク安全・信頼性基準その他の国内・国際の公表されている情報セキュリティーに関する基準を活用して、各電気通信事業者が適切な内部規程・マニュアルを策定し、実施することが必要である。<br>なお、事業用電気通信設備（電気通信回線設備及び基礎的電気通信役務を提供する電気通信事業の用に供する電気通信設備）に関する技術的保護措置については、事業用電気通信設備を設置する電気通信事業者に対し、事業用電気通信設備規則（昭和６０年郵政省令第３０号）に定める技術基準の適合維持義務が課されている（電気通信事業法第４１条）ことにも留意する必要がある。<br>(3) 組織的保護措置とは、<br>① 安全管理に関する従業者・委託先の責任と権限を明確に定めること<br>② 安全管理に関する内部規程・マニュアルを定め、それらを従業者に遵守させるとともに、その遵守の状況について適切な監査を行うこと<br>③ 従業者・委託先と秘密保持契約を締結すること等により安全管理について従業者・委託先を適切に監督すること<br>④ 安全管理について従業者に対し必要な教育研修を行うこと<br>などの人的・組織的な措置を指すが、これらの事項については、次条及び第１３条に詳細な規定がおかれているので、それらの規定の解説を参照されたい。 |

| | |
|---|---|
| 持ち出した個人情報の安全性を確保するためには、リスクの評価、リスクに対応するために必要とされる措置の検討・決定、決定した措置の適切な運用という手順で対策を行うことが必要である。<br>まず、リスクの評価に当たっては、個人情報の持出し時に想定される具体的なリスクを網羅的に評価することが必要である。<br>次に、措置の検討・決定に当たっては、技術的保護措置と組織的保護措置との双方についての検討が必要である。技術的保護措置については、個々の技術的保護措置の特性を把握しリスクに適切に対応できる具体的な措置を選択することが必要である。その際には、複数の措置（パーソナルコンピュータの起動時等での個人認証、外部媒体の接続制限、ウイルス侵入による情報漏えいに備えた最新のセキュリティー水準維持、高度な暗号化措置及び適切な復号鍵の管理、通信経路の暗号化、社内サーバにおける端末認証等）を適切に組み合わせることが重要である。また、講じようとする技術的保護措置の技術的に最も弱い部分を確認すること、利便性、安全性及び導入コストを勘案することが重要である。組織的保護措置については、技術的保護措置が適切に運用されるよう、安全管理措置に関する内部規程の整備や従業員への周知等を行うことが必要である。<br>さらに、決定した措置の適切な運用に当たっては、定期的な監査や従業員に対する定期的な研修の実施等に努めるとともに、リスクの状況について適宜に見直しを行うことが必要である。<br>なお、技術的保護措置を講じていたとしても、業務上必要な分量や種類を超えた個人情報を持ち出すことは避け、必要最低限の範囲にするべきである。また、漏えいした場合に本人の権利利益の侵害の程度が大きい個人情報については、安易に外部に持ち出さないこととするとともに、持ち出す必要がある場合は、より高い安全性が確保されるような技術的保護措置を講ずることが必要である。 | |

| 改正案 | 現行 |
| --- | --- |
| （漏えい等が発生した場合の対応）<br>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。<br>２　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、この限りでない。<br>３　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もって代えることができる。 | （漏えい等が発生した場合の対応）<br>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。<br>２　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。<br>３　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。 |
| （解説）<br>(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 | （解説）<br>(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。<br>　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。<br>(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。<br>　「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①ノートブック型のパーソナルコンピュータ、②携帯電話端末、ＰＤＡ等の通信端末機器、③ＵＳＢ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。<br>　「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。<br>①　高度な暗号化措置が講じられていること<br>　　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。<br>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<br>　　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。 | 連絡先が不明である場合は、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。<br>　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。 |

| | |
|---|---|
| （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<br>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。<br>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。<br>（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。<br>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。 | |
| (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。<br>同項ただし書は、(2)と同様の考え方によるものである。 | (2) 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。 |
| (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。 | (3) 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、四半期内に認知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。<br>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。<br>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。 | |