情報取扱規程記載マニュアル

令和 6 年 1 月 17 日

総務省 総合通信基盤局 電気通信事業部 利用環境課

はじめに

情報通信技術を活用したサービスの多様化やグローバル化に伴い、情報の漏えい・不適正な取扱い等のリスクが高まる中、事業者が保有するデータの適正な取扱いが一層必要不可欠となっている。このような状況を踏まえ、令和4年6月には、大規模な事業者が取得する利用者情報について適正な取扱いを義務づけた特定利用者情報規律等を内容とする改正電気通信事業法が成立し、令和5年6月に施行されたところである。

電気通信事業法（昭和 59 年法律第 86 号）第 27 条の5の規定に基づき、特定利用者情報を適正に取り扱うべき電気通信事業者として指定された電気通信事業者（以下「指定電気通信事業者」という。）は、特定利用者情報の適正な取扱いを確保するため、次に掲げる事項に関する規程を定め、指定の日から3か月以内に、総務大臣へ届け出ること等が義務づけられている。

（1）特定利用者情報の漏えい、滅失又は毀損の防止その他の当該特定利用者情報の安全管理に関する事項
（2）特定利用者情報の取扱いを第三者に委託する場合における当該委託を受けた者に対する監督に関する事項
（3）情報取扱方針の策定及び公表に関する事項
（4）特定利用者情報の取扱状況の評価に関する事項
（5）特定利用者情報を取り扱う従事者に対する監督に関する事項

本文書は、情報取扱規程の各事項に関する具体的な例等を示すことで、指定電気通信事業者が情報取扱規程を作成する際の参考とすることができるよう作成したものである。なお、本文書における例示等は、情報取扱規程に記載することが求められる事項について、その一例を示したものであり、前述の5つの事項が満たされていれば、本文書における具体例の記載を求めるものではない。

また、本文書については、指定電気通信事業者における特定利用者情報の漏えいの発生状況や利用者情報の取扱いの状況等に応じて、適時見直しを図ることとする。

1．特定利用者情報の漏えい、滅失又は毀損（以下「漏えい等」という）の防止その他の当該特定利用者情報の安全管理に関する次に掲げる事項

（1）組織的安全管理措置に関すること

①組織体制の整備

- 特定利用者情報の取扱いに関する責任者（特定利用者情報統括管理者）の設置及び責任の明確化、特定利用者情報を取り扱う従事者及びその役割の明確化
- 上記の従事者が取り扱う特定利用者情報の範囲の明確化
- 電気通信事業法や情報取扱規程、情報取扱方針に違反している事実又は兆候を把握した場合の責任者への報告連絡体制
- 特定利用者情報の漏えい等事案の発生又は兆候を把握した場合の責任者への報告連絡

体制

・ 特定利用者情報を複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化

②特定利用者情報の取扱いに係る適正な運用

・ 特定利用者情報の取扱いに係る適正な運用を確保するため、例えば次のような項目に関して、システムログその他の特定利用者情報の取扱いに係る記録の整備や業務日誌の作成等を通じて、特定利用者情報の取扱いの検証を可能とすることが考えられる。
  - 特定利用者情報の利用状況
  - 特定利用者情報が記載又は記録された書類・媒体等の持ち運び等の状況
  - 特定利用者情報の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。）
  - 特定利用者情報を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）
・ 特定利用者情報の取扱いに関する留意事項等をまとめたマニュアル等の整備

③特定利用者情報の取扱状況を確認する手段の整備

・ 例えば次のような項目をあらかじめ明確化しておくことにより、特定利用者情報の取扱状況を把握可能とすることが考えられる。
  - 特定利用者情報の項目
  - 責任者・取扱部署
  - 利用目的
  - アクセス権を有する者　等

④漏えい等事案に対応する体制の整備

・ 漏えい等事案の発生時に、例えば次のような対応を行うための体制を整備することが考えられる。
  - 事実関係の調査及び原因の究明
  - 総務省への報告
  - 再発防止策の検討及び決定　等

(2) 人的安全管理措置に関すること

①従事者の教育

・ 特定利用者情報の取扱いに関する留意事項について、従事者に定期的な研修等を行う。
・ 特定利用者情報についての秘密保持に関する事項を就業規則等に盛り込む。

②非開示契約

・ 雇用契約時における従業員との非開示契約の締結や秘密保持等に関する誓約書の提出、委託契約等（派遣契約を含む）における委託元と委託先間での非開示契約の締結。
・ 特定利用者情報に関する非開示の義務を、就業規則等の社内規程に規定。

(3) 物理的安全管理措置に関すること

①特定利用者情報を取り扱う区域の管理

・ 入退室管理及び持ち込む機器等の制限等
  - 入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。
・ 壁又は間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による特定利用者情報の閲覧等の防止。

②機器及び電子媒体等の盗難等の防止

・ 特定利用者情報を取り扱う機器、特定利用者情報が記録された電子媒体又は特定利用者情報が記載された書類等を、施錠できるキャビネット・書庫等に保管する。
・ 特定利用者情報を取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。

③電子媒体等を持ち運ぶ場合の漏えい等の防止

・ 特定利用者情報の持ち出し時に想定される具体的なリスクを網羅的に評価し、リスクに対応するために必要とされる措置（パソコン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）を検討・決定し、決定した措置の適切な運用を行う。
・ 持ち運ぶ特定利用者情報の暗号化、パスワードによる保護等を行った上で電子媒体に保存する。
・ 封緘、目隠しシールの貼付けを行う。
・ 施錠できる搬送容器を利用する。

④特定利用者情報の削除及び機器、電子媒体等の廃棄

・ 焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。
・ 情報システム（パソコン等の機器を含む。）において、特定利用者情報を削除する場合、容易に復元できない手段を採用する。
・ 特定利用者情報が記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。

(4) 技術的安全管理措置に関すること

①アクセス制御

- 特定利用者情報を取り扱うことのできる情報システムを限定する。
- 情報システムによってアクセスすることのできる特定利用者情報を限定する。
- ユーザーID に付与するアクセス権により、特定利用者情報を取り扱う情報システムを使用できる従事者を限定する。

②アクセス者の識別と認証

- 特定利用者情報を取り扱う情報システムにアクセスをする際は、ユーザーID、パスワード、磁気・IC カード等によりアクセス者の識別と認証を行う。

③外部からの不正アクセス等の防止

- 情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスや DDoS 攻撃等のサイバー攻撃への対策を行う。
- 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。
- 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。
- ログ等の定期的な分析により、不正アクセス等を検知する。

④情報システムの使用に伴う漏えい等の防止

- 情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。
- 特定利用者情報を含む通信の経路又は内容を暗号化する。
- 移送する特定利用者情報について、パスワード等による保護を行う。

(5) 特定利用者情報の適正な取扱いに影響を及ぼすおそれのある外国の制度の把握の体制に関すること

- 外部による調査結果※を適時に確認することに関する事項
- 社内における専門の調査チームの組成に関する事項
- 外部専門家の起用に関する事項

※ 特定利用者情報の適正な取扱いに影響を及ぼすおそれのある外国の制度について、令和５年度に、渥美坂井法律事務所において総務省の請負調査を実施。指定電気通信事業者等は、主管課に問い合わせることにより当該調査の結果を入手可能。ただし、調査結果の内容は総務省の公式見解を示すものではない。

２．特定利用者情報の取扱いを第三者に委託する場合における当該委託を受けた者に対する監督に関する次に掲げる事項

⑴ 委託先の選定の方法に関すること

・ 上記1⑴～⑷に定める各項目と同等の措置が委託先において確実に実施されることの確認方法に関する事項。

⑵ 委託契約において定める特定利用者情報の取扱いに関すること

・ 委託先の安全管理措置、秘密保持、再委託の条件、委託契約終了時の特定利用者情報の取扱い、契約内容が遵守されなかった場合の措置、その他の特定利用者情報の取扱いに関する事項。

⑶ 委託先（再委託先、再々委託先等を含む。）における特定利用者情報の取扱状況の把握の体制及び方法に関すること

・ 委託先に対する定期的監査の実施、監査結果を踏まえた委託契約の見直しに関する事項。
・ 再委託先（再々委託先等を含む）における情報の取扱状況の把握方法に関する事項。

３．情報取扱方針の策定及び公表に関する事項

・ 情報取扱方針の策定組織に関する事項。
・ 情報取扱方針の公表方法（公表場所等）に関する事項。

４．特定利用者情報の取扱状況の評価（第 27 条の9第 1 項）に関する次に掲げる事項

⑴ 当該評価の実施並びに当該評価の結果の情報取扱規程及び情報取扱方針への反映の体制に関すること

・ 評価の実施体制（実施部門及び社外専門家の関与の有無等）に関する事項。
・ 評価結果の情報取扱規程及び情報取扱方針への反映体制（反映の必要性の判断方法、反映作業の実施部門等）に関する事項。

⑵ 当該評価を行う項目、方法及び頻度に関すること

・ 評価項目（直近の事業年度における情報取扱規程及び情報取扱方針の遵守状況、直近の事業年度における特定利用者情報の漏えいの発生原因・講じられた再発防止策の有効性等）に関する事項。
・ 評価方法（評価基準等）に関する事項。
・ 評価時期及び頻度に関する事項。

５．特定利用者情報を取り扱う従事者に対する監督に関する事項

・ 特定利用者情報を取り扱う従事者の監督体制及び監督方法（アクセス管理等）に関する事

項。

・ 上記の従事者に対する教育研修等の内容（情報取扱規程やマニュアル等の周知等）、頻度に関する事項。

以上