

ICTサービスにおける 個人情報・利用者情報等の取扱いに関する課題

事務局

- 「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」や同ガイドラインの解説については、ICTサービスを取りまく最近の動向等を踏まえ、速やかに以下の内容等について見直しを行うべきではないか。

【「ガイドラインの共通化の考え方について」の改定を踏まえての対応】

- ・ 第三者からの適正な情報取得の徹底
- ・ 社内の安全管理措置の強化
- ・ 委託先の管理の強化

【消費者保護の充実やセキュリティ対策の強化等の要請を踏まえての対応】

- ・ 通信履歴(ログ)の保存の在り方についてのより具体的で明確な考え方の提示

- インターネット上での個人情報・利用者情報等の取扱いについて、近年のインターネット利用の進展や高度化・多様化に伴い、様々な課題が生じており、現行制度、関係事業者・団体による取組、海外動向等も踏まえつつ、これらの問題に対する事実関係や論点を整理し、今後の課題や取組の方向性について検討していく必要があるのではないか。

- その他ICTサービスにおける個人情報・利用者情報等の取扱いに関して整理すべき事項があれば、併せて検討すべきではないか。

(参考) 今後、総務省において実施を予定している個人情報・利用者情報等の取扱いに関する取組

○「位置情報プライバシーレポート」を踏まえた位置情報の適切な利活用についての実証

○スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る技術的検証等の実証

- 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等の見直し
- インターネット上での個人情報・利用者情報等の取扱いの在り方

第三者からの情報の取得

個人情報保護法の規定

(適正な取得)

第17条 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

現行ガイドラインの規定・解説

(適正な取得)

第7条 電気通信事業者は、偽りその他不正の手段により個人情報を取得しないものとする。

(解説)

個人情報の取得は、適法かつ公正な手段により行わなければならない、偽りその他不正の手段によることは許されない。

検討事項

第三者からの適正な情報取得の徹底について、「ガイドラインの共通化の考え方について」の改定(資料6参照)等を踏まえて、ガイドライン及びその解説について見直しを行う。

(参考)

「ガイドラインの共通化の考え方について」(主な関連部分抜粋)(資料6及び参考資料4参照)

第三者からの提供(法第23条第1項各号に掲げる場合並びに個人情報の取扱いの委託、事業の承継及び共同利用に伴い、個人情報を提供する場合を除く。)により、個人情報(施行令第2条第2号に規定するものから取得した個人情報を除く。)を取得する場合には、提供元の法の遵守状況(例えば、オプトアウト(7.(3)の規定(法第23条第2項・第3項)参照)、利用目的、開示手続、問合せ・苦情の受付窓口を公表していることなど)を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得の経緯を示す契約書等の書面の点検又はこれに代わる合理的な方法により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

なお、経済産業省のガイドラインの改定について、資料5の6ページ参照

安全管理措置

個人情報保護法の規定

(安全管理措置)

第20条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない

現行ガイドラインの規定・解説

(安全管理措置)

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。

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)

(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。

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。

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。

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。

(2) 技術的保護措置とは、

- 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)
- 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)
- 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。

現行ガイドラインの解説

(第11条解説の続き)

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。

(3) 組織的保護措置とは、

- 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
- 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
- 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
- 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

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。

(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。

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。

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。

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。

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。

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。

現行ガイドラインの規定・解説

(個人情報保護管理者)

第13条 電気通信事業者は、個人情報保護管理者(当該電気通信事業者の個人情報の取扱いに関する責任者をいう。)を置き、このガイドラインを遵守するための内部規程の策定、監査体制の整備及び当該電気通信事業者の個人情報の取扱いの監督を行わせるものとする。

(解説)

個人情報保護措置の実施に関する責任の所在を明確にし、第11条の安全管理措置の実施その他の個人情報の適正な取扱いについて電気通信事業者の内部における責任体制を確保するため、電気通信事業者は、当該電気通信事業者の個人情報の適正な取扱いの確保について必要な権限を有する者(個人情報保護管理者)を置いて、個人情報保護管理者において責任をもって必要な個人情報保護の取扱いの監督等を行わせるものとした。

検討事項

社内の安全管理措置の強化について、「ガイドラインの共通化の考え方について」の改定(資料6参照)等を踏まえて、ガイドライン及びその解説について見直しを行う。

(参考)

「ガイドラインの共通化の考え方について」(主な関連部分抜粋)(資料6及び参考資料4参照)

[特に、事業者の内部又は外部からの不正行為による個人データの漏えい等を防止するための手法として、例えば次のような措置を講じることが望ましい。]

① 責任の所在の明確化のための措置

(例)

- ・ 個人データの安全管理の実施及び運用に関する責任及び権限を有する個人情報保護管理者の設置(例えば、役員などの組織横断的に監督することのできる者を任命する)
- ・ 事業者内の個人データの取扱いの点検・改善等の監督を行う部署の設置
- ・ 事業者内の個人データの取扱いの点検・改善等の監督を行う合議制の委員会の設置

② 新たなリスクに対応するための、安全管理措置の評価、見直し及び改善に向けた監査実施体制の整備

(例)

- ・ 個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者による事業者内の対応の確認(必要に応じ、外部の知見を有する者を活用し確認させることを含む。)

③ 漏えい等に早期に対処するための体制整備

(例)

- ・ 漏えい等が発生した場合又は発生のおそれがある場合の連絡体制の整備

- ④ 不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性に基づく限定
(例)
 - ・ スマートフォン、パソコン等の記録機能を有する機器の接続の制限及び機器の更新への対応
- ⑤ 入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館（室）管理の実施
(例)
 - ・ 入退館（室）の記録の保存
- ⑥ 盗難等の防止のための措置
(例)
 - ・ カメラによる撮影や作業への立会い等による記録又はモニタリングの実施
 - ・ 記録機能を持つ媒体の持込み・持出し禁止又は検査の実施
- ⑦ 情報システムからの漏えい等を防止するための技術的安全管理措置
(例)
 - ・ 個人データへのアクセスにおける識別と認証
 - ・ 個人データへのアクセス制御
 - ・ 個人データへのアクセス権限の管理
 - ・ 個人データへのアクセスや操作の記録及び不正が疑われる異常な記録の存否の定期的な確認
 - ・ 情報システムへの外部からのアクセス状況の監視及び当該監視システムの動作の定期的な確認
 - ・ ソフトウェアに関する脆弱性対策（セキュリティパッチの適用、当該情報システム固有の脆弱性の発見及びその修正等）]

なお、経済産業省のガイドラインの改定について、資料5の4ページ参照

委託先の監督の強化①

委託先の監督

個人情報保護法の規定

(委託先の監督)

第22条 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

現行ガイドラインの規定・解説

(従業者及び委託先の監督)

第12条 1、2(略)

3 電気通信事業者は、個人情報の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人情報の安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うものとする。

4 電気通信事業者は、前項の場合は、個人情報を適正に取り扱おうと認められる者を選定し、委託契約において、安全管理措置、秘密保持、再委託の条件(再委託を許すかどうか並びに再委託を許す場合は再委託先の選定及び再委託先の監督に関する事項等)その他の個人情報の取扱いに関する事項について適正に定めるものとする。

5 電気通信事業に従事する者及び電気通信事業者から委託された個人情報の取扱いに係る業務に従事する者は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせないものとし、また、不当な目的に使用しないものとする。その職を退いた後においても同様とする。

(解説) (1) (2) 略

(3) 第3項は、電気通信事業者が個人情報の取扱いを他の者に委託する場合に、前条の安全管理措置のうちの組織的保護措置の一環として、特に電気通信事業者はその委託先に対して必要かつ適切な監督を行う責任があることを規定したものである。「委託」とは、契約の形態・種類を問わず、電気通信事業者が他の者に個人情報の取扱いの全部又は一部を行わせることを内容とする契約の一切を含むものである。具体的な委託先としては、契約代理業者(電気通信事業者の電気通信役務の提供に関する契約の締結の媒介、取次ぎ又は代理を業として行う者)や電気通信事業者の顧客の個人情報の入力、編集、出力等の処理を行う者や料金の回収・決済を代行する者などがあげられる。

(4) 第4項は、第3項の委託に当たって、個人情報を適正に取り扱おうと認められる者を選定すること、及び、委託契約において、安全管理措置、秘密保持、再委託の条件(再委託を許すかどうか並びに再委託先を許す場合は再委託先に個人情報を適正に取り扱っていると認められることを選定すること及び再委託先の監督に関する事項等。なお、二段階以上の委託を許す場合は同様に再々委託先等の選任監督に関する事項を定める必要がある。)、委託契約終了時の個人情報の返却等その他の個人情報の取扱いに関する事項を適正に定めることを規定したものである。

(5) 第5項は、電気通信事業法第4条第2項において、電気通信事業に従事する者に対し、「通信に関して知り得た他人の秘密」を守るべき義務が課されているが、個々の通信に関係ない個人情報については、かかる守秘義務は及ばないと考えられる。しかし、個人情報保護の観点からは、同様に保護することが適当であることから、電気通信事業に従事する者(電気通信事業者及びその従業者)及び電気通信事業者から委託された個人情報の取扱いの業務に従事する者(受託者及びその従業者)について、個人情報を適正に取り扱うべき責務があることを明らかにしたものである。

委託先の監督の強化②

検討事項

委託先の監督の強化について、「ガイドラインの共通化の考え方について」の改定(資料6参照)等を踏まえてガイドライン及びその解説の見直しを行う。

(参考)

「ガイドラインの共通化の考え方について」(主な関連部分抜粋)(資料6及び参考資料4参照)

[② [〇〇関係事業者] は、委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第20条で求められるものと同等であることを確認するため、[以下の項目が、委託する業務内容に応じて、確実に実施されることについて、] 委託先の体制、規程等の確認に加え、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行った上で、個人情報保護管理者等が、適切に評価することが望ましい。]

[③ [〇〇関係事業者] は、委託契約等において次に示す事項について定めることが望ましい。

ア 委託先の個人データの取扱いに関する事項

(例)

- ・ 委託先において個人データを取り扱う者(委託先で作業する委託先の作業員以外の者を含む)を明確にすること
- ・ 委託先において講ずべき安全管理措置の内容

イ 委託先の秘密の保持に関する事項

ウ 委託された個人データの再委託に関する事項

(例)

- ・ 再委託の可否及び再委託を行うに当たっての委託元への文書による事前報告又は承認

エ 契約終了時の個人データの返却等に関する事項

オ 契約内容が遵守されなかった場合の措置

(例)

- ・ 安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項]

[④ 委託先における委託された個人データの取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

委託先が再委託を行おうとする場合は、委託元は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先に事前報告又は承認手続を求める、直接又は委託先を通じて定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、再委託先が法第20条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。]

なお、経済産業省のガイドラインの改正について、資料5の5ページ参照

電気通信事業法の規定

(秘密の保護)

第4条 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

通信履歴(ログ)について

- 通信履歴 (ログ) とは、利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう。
- 「通信の秘密」の範囲には、個別の通信に係る通信内容のほか、個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知されるような事項全てが含まれる。よって、通信履歴 (ログ) も通信の秘密として保護される。

(参考1) 東京地裁判決平成14年4月30日

「電気通信事業法第104条の「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」

(参考2) 内閣法制局見解昭和57年7月15日

「一般に、通信の当事者の居所・氏名・発信地・受信地・通話回数・通信年月日などは通信の意味内容をなす者ではないが、通信そのものの構成要素であり、実質的にこれらの事項を知られることによって、通信の意味内容が推知されることもあり得るから、これらの事項も通信の秘密として保護される対象に含まれると解されている。」

通信履歴(ログ)の保存について

- 通信履歴 (ログ) を記録する行為は通信の秘密の知得と考えられ、通信の秘密の侵害に該当する。通信履歴 (ログ) の保存は、通信履歴 (ログ) を記録しその記録した状態を継続する行為であることから、通信履歴の保存も通信の秘密を侵害していると考えられる。
- 通信履歴の保存は、通信の秘密を侵害していると考えられることから、現行法上、認められるのは、利用者の同意がある場合のほか、違法性阻却事由のある場合、具体的には、電気通信事業者の正当業務行為となる場合と考えられ、従来、課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合に行われてきた。

現行ガイドラインの規定・解説

(通信履歴)

第23条 電気通信事業者は、通信履歴(利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であつて通信内容以外のものをいう。以下同じ。)については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。

2 電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合、正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合を除いては、通信履歴を他人に提供しないものとする。

(解説)

(1) 通信履歴は、通信の構成要素であり、電気通信事業法第4条第1項の通信の秘密として保護される。したがって、これを記録することも通信の秘密の侵害に該当し得るが、課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には正当業務行為として少なくとも違法性が阻却されると考えられる。

(2) (3) (4) 略

(5) いったん記録した通信履歴は、第10条の規定に従い、記録目的に必要な範囲で保存期間を設定することを原則とし、保存期間が経過したときは速やかに通信履歴を消去(個人情報本人が識別できなくすることを含む。)する必要がある。この保存期間については、提供するサービスの種類、課金方法等により各電気通信事業者ごとに、また通信履歴の種類ごとに異なり得るが、その趣旨を没却しないように限定的に設定すべきであると考えられる。また、保存期間を設定していない場合には、記録目的を達成後、速やかに消去する必要がある。ただし、法令の規定による場合その他特別の理由がある場合には例外的に保存し続けることができると考えられる。自己又は第三者の権利を保護するため緊急行為として保存する必要がある場合は、その他特別な理由がある場合として保存が許されると考えられる。

検討事項

ICTサービスが高度化・多様化する中、消費者保護の見直し・充実の観点からの利用者からの問合せ・苦情に対する対応などについての強化や、適正なサービスの提供やネットワークの運営の確保、セキュリティ対策の強化などに関する要請が最近とみに高まっており、これらの要請に対し必要となる通信履歴(ログ)の保存の在り方について、利用者の表現行為やプライバシーへの関わり方の程度などにも配慮しつつ、関係事業者においてより判断を行いやすくなるよう、より具体的で明確な考え方が提示されることが必要ではないか。

- 「サイバーセキュリティ戦略」(平成25年6月10日情報セキュリティ政策会議決定)

2015年度までの3年間、以下に掲げる取組を進めることとする。(略)

⑤サイバー空間の犯罪対策

サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログの保存期間、一般利用者としての国民の多様な意見等を勘案した上でサイバー犯罪における捜査への利用の在り方について検討する。

- 「「世界一安全な日本」創造戦略」(平成25年12月10日犯罪対策閣僚会議決定、閣議決定)

通信履歴(ログ)の保存の在り方及び新たな捜査手法についての検討

サイバー犯罪に対する事後追跡可能性を確保するため、「サイバーセキュリティ戦略」(平成25年6月10日情報セキュリティ政策会議決定)に基づき、関係事業者における通信履歴等の保存の在り方について、所要の措置を講ずることができるよう検討を行い、可能な範囲で速やかに一定の結論を得る。

- 「私事性的画像記録の提供等による被害の防止に関する法律」(平成26年11月27日法律第126号)

附則第二条

政府は、インターネットを利用した私事性的画像記録の提供等に係る被害回復及び処罰の確保に資するため、この法律の施行後二年以内に、外国のサーバーを経由するなどした私事性的画像記録の提供に関する行為者の把握及び証拠の保全等を迅速に行うための国際協力の在り方について検討するとともに、関係事業者における通信履歴等の保存の在り方について検討を加え、その結果に基づいて必要な措置を講ずるものとする。

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等の見直し

インターネット上での個人情報・利用者情報等の取扱いの在り方

○プロバイダ責任制限法の特例規定

ネット選挙運動解禁に伴うプロバイダ責任制限法の改正（平成25年4月19日公布）

- ・選挙運動期間中に配布された選挙運動等に使用する情報の流通により自己の名誉を侵害されたとする候補者等からプロバイダ等に削除の申出があった場合、プロバイダ等から発信者に対する削除同意照会期間が、通常の「7日」から「2日」に短縮等された（プロバイダ責任制限法3条の2）。

私事性的画像記録の提供等による被害の防止に関する法律の制定（平成26年11月27日公布）

- ・いわゆるリベンジポルノ画像等がインターネット上に流通することにより、被害者が長期にわたり多大な精神的被害を受けるという事案が問題化。このような被害の発生等を防止することを目的とした「私事性的画像記録の提供等による被害の防止に関する法律」が成立。
- ・プロバイダ責任制限法の特則として、私事性的画像記録に係る情報の流通により名誉または私生活の平穏を侵害されたとする申出者からプロバイダ等に削除の申出があった場合、プロバイダ等から発信者に対する削除同意期間が通常の「7日」から「2日」に短縮された（私事性的画像記録の提供等による被害の防止に関する法律第4条）。

私事性的画像記録の提供等による被害の防止に関する法律概要

平成26年11月27日公布、同日施行（第3条は12月17日、第4条は12月27日施行。）

1 目的(第1条)

私事性的画像記録の提供等の処罰・プロ責法の特例・支援体制整備 等 ⇒ 個人の名誉・私生活の平穩の侵害による被害の発生・拡大を防止

2 定義(第2条)

●「私事性的画像記録」（電子情報）・「私事性的画像記録物」（有体物）★児童ポルノ禁止法の「児童ポルノ」の定義に倣ったもの
＝①～③のいずれかに掲げる人の姿態が撮影された画像(※)に係る記録・物 ※本人が第三者に見られることを認識した上で撮影を許可した画像を除く

- ①性交又は性交類似行為に係る人の姿態
- ②他人が人の性器等を触る行為又は人が他人の性器等を触る行為に係る人の姿態であって性欲を興奮させ又は刺激するもの
- ③衣服の全部又は一部を着けない人の姿態であって、殊更に人の性的な部位が露出され又は強調されているものであり、かつ、性欲を興奮させ又は刺激するもの

3 罰則(第3条)

(1) 公表罪

第三者が撮影対象者を特定することができる方法で、私事性的画像記録(物)を不特定若しくは多数の者に提供し、又は公然と陳列した者 ⇒3年以下の懲役又は50万円以下の罰金

(2) 公表目的提供罪

(1)の行為をさせる目的で、私事性的画像記録(物)を提供した者 ⇒1年以下の懲役又は30万円以下の罰金

4 プロバイダ責任制限法の特例(画像の削除)(第4条)

【現状のプロバイダ責任制限法】

- ◎違法性が明らかな場合など ⇒ガイドラインや契約約款により即時削除
- プロバイダ等が権利侵害を判断できる場合 ⇒即時削除(法による免責)
- △プロバイダ等が権利侵害を判断できない場合 ⇒①発信者に対して削除に同意するか照会→②7日経過しても不同意の申出がない→③削除(法による免責)

⇒ 同意照会に関し7日を2日に短縮する特例を創設(公職の候補者等に係る特例を参考にしたもの)。被害者死亡の場合には遺族が申出可

5 支援体制の整備等(第5条・第6条)

- 支援体制の整備等
被害者が告訴などを行いやすくするために必要な体制の充実、削除の申出先、申出方法等についての周知を図るための広報活動等の充実 等
- 被害の発生を未然に防止するための教育及び啓発

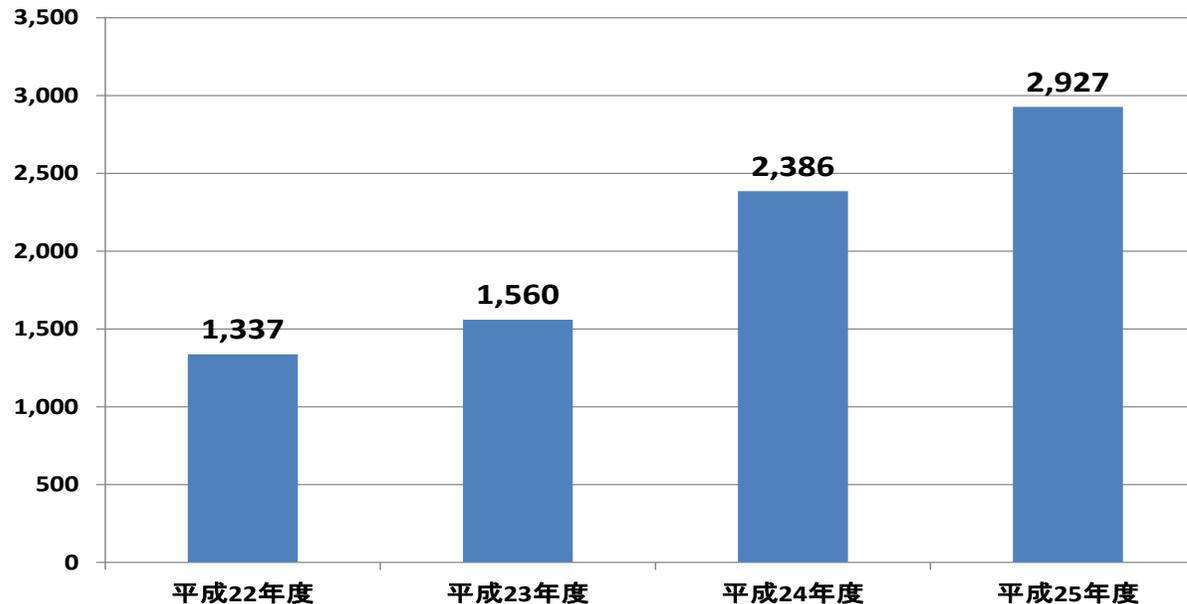
6 その他(附則)

- 被害回復及び処罰の確保に資する国際協力の在り方等に関する検討、この法律の見直しに関する検討等

違法・有害情報相談センターにおける相談件数の増加

・総務省の運営する違法・有害情報相談センターで受け付けている相談の件数は年々増加傾向にあり、平成25年度の相談件数は、平成22年度の相談件数の2倍以上に増加している。

〈平成22年度：1,337件、平成23年度：1,560件、平成24年度：2,386件、平成25年度：2,927件〉



検討課題

インターネット上での個人情報・利用者情報等の取扱いについては、近年のインターネット利用の進展や高度化・多様化に伴い、様々な課題が生じており、現行制度、関係事業者・団体による取組、海外動向等も踏まえつつ、これらの問題に対する事実関係や論点を整理し、今後の課題や取組の方向性について検討していく必要があるのではないか。

EU個人データ保護規則案(2012年1月25日欧州委員会提案 2014年3月12日欧州議会修正案可決)

第17条 消去する権利 (right to erasure) (当初案「忘れられる権利及び消去する権利」(right to be forgotten and to erasure))
本人が求めた場合、自己の個人データを消去する権利を有する。さらにこの権利を強めるため、本人からデータの消去の求めがあった企業は、そのデータが他の事業者複製されている場合は、データの消去要請があったことをその事業者に対して通知しなければならない。通知を受け取った事業者には、そのデータを消去する義務が発生する。

「第29条作業部会」による、グーグルスペイン社事件先行判決の執行に係るガイドラインの発表(2014年11月26日)

EU加盟国当局及び欧州委員会からなる諮問機関「第29条作業部会」は、主要検索事業者からのヒアリング等を踏まえて法的検討を行い、2014年11月26日、グーグルスペイン社事件の先行判決の解釈指針と加盟国当局の対応指針を示したガイドラインを発表。

- ・ 検索事業者は「データ管理者」(現行指令第2条)と見なされ、その結果、データ主体(個人)による「違法情報の消去を求める権利」(同12条)に服する(ただし、「知る権利」との利益衡量を行う)。
- ・ 検索事業者により削除を拒否された個人に対する加盟国当局の対応について、共通の基準となる考え方として、人名に基づく検索結果か、公共人か、未成年者か、検索結果は正確か、検索結果は、データ主体に関連しているか、センシティブ情報か、検索結果は最新の情報か、偏見が生じているか、リスクを生じているか、データ公開の意図は何か、リンク元サイトに報道目的があるか、リンク元サイトに公開の義務があるか、刑事犯罪に関連しているか、などを列挙。

〔グーグルスペイン社事件先行判決(2014年5月13日)〕

EU司法裁判所は、スペイン裁判所の意見照会を受けて、データ主体は、一定の場合に、検索事業者に対して、検索リストから自己に関する過去の情報の削除を求めることができるとする先行判決を下した。

＜事案の概要＞

スペイン人男性が、Googleの検索エンジンに自分の名前を入れて検索したところ、自分に関する情報を含む1998年の新聞記事が表示された。当該記事は男性の債務超過に伴う不動産強制競売に関するものだったが、既に本件は解決済みであることからGoogle社(西、米)への検索結果の削除を求めた。

cf: なお、日本の裁判例においても、グーグル社に対して検索結果の削除が求められた事例において、「検索結果から『男性は素行が不適切な人物』との印象を与え、実害も受けた」として検索結果の一部の削除を認める仮処分決定(平成26年10月9日東京地裁決定判例集未搭載)がなされている(日本経済新聞平成26年10月10日紙面参照)。