資料１

「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」の改正について（案）

（案）

平成 27 年３月

ＩＣＴサービス安心・安全研究会

個人情報・利用者情報等の取扱いに関するＷＧ

Ⅰ　検討の背景と経緯

平成 26 年夏、株式会社ベネッセコーポレーションからシステム開発・管理の委託を受けていた企業に従事する技術者が、平成 25 年夏以降、2895 万件の同社の顧客情報を持ち出し、名簿業者に売却していた事実（以下「本情報漏えい事案」という。）が発覚した。

経済産業省では、同社からの報告を踏まえ、同年９月 26 日、同社に対して、個人情報の保護に関する法律（以下「個人情報保護法」という。）に基づき、①委託先も含めた個人情報の保護に関する実施体制の明確化、②システムセキュリティ対策の具体化を内容とする勧告を行った。

また、本情報漏えい事案を踏まえ、広く産業界に対し、個人情報の管理に万全を期すことを促す観点から、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」について、（１）社内の安全管理措置の強化、（２）委託先等の監督の強化、（３）第三者からの適正な情報取得の徹底に関するぞれぞれの取組の充実・強化を図ることを要点とした改正を行い、同年 12 月 12 日に公表した。

一方、こうした動きと呼応して、同年９月 30 日、消費者庁では、個人情報保護関係省庁連絡会議を開催し、関係省庁の間で、①個人情報の適正な取得、②安全管理措置、③委託先の監督等、個人情報保護法の遵守を徹底するため、事業等分野ごとのガイドラインの改定など必要な措置を講じる旨の申合せを行った。

その上で、消費者庁は、同年 11 月 19 日、「ガイドラインの共通化の考え方について」（以下「共通化の考え方」という。）を改定し、本情報漏えい事案を踏まえ、各府省における各分野の個人情報保護ガイドラインの改定に当たり盛り込むべき事項等の考え方を明らかにした。

これを踏まえ、総務省では、「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」（同ガイドラインの解説を含め、以下「本ガイドライン」という。）の改正を検討することとし、具体的な改正内容については、ＩＣＴサービス安心・安全研究会に新たに設置する「個人情報・利用者情報等の取扱いに関するＷＧ」（以下「本ＷＧ」という。）において検討することとした。

また、本ＷＧでの本ガイドラインの改正の検討に際しては、本ガイドライン

の解釈・運用に当たって早期の検討を求められていた通信履歴の保存［や位置情報の利用］といった課題についても、併せて行うこととした。

本WGは平成 26 年 12 月４日に開催されたＩＣＴサービス安心・安全研究会において設置が承認された。本WGの第１回会合は平成 27 年１月８日に開催され、検討課題等についての議論を行った。第２回会合は同年２月５日に開催され、電気通信サービスにおける個人情報や通信履歴の取扱いに関する実態や本ガイドラインの改正に関する意見について、一般社団法人電気通信事業者協会及び一般社団法人日本インターネットプロバイダー協会から聴取した。［そして、第３回会合は同年３月２日に開催され、本報告書案について議論を行った。］

以上の検討を踏まえ、本WGでは、本報告書案の取りまとめを行ったものである。本WGでは、本報告書案に対するパブリックコメント手続の結果を踏まえ、最終的な取りまとめを行う予定である。総務省においては、本報告書の最終取りまとめを踏まえ、速やかに本ガイドラインの改正を行うことを期待する。

II　改正の内容

本ガイドラインの改正については、本WGでの検討の趣旨を踏まえ、以下の内容とすることが適当であると考えられる。

１　第７条（適正な取得）について

（１）検討の趣旨

共通化の考え方では、本情報漏えい事案を踏まえ、個人情報の適正な取得を目的として、第三者からの提供により個人情報を取得する場合には、提供元の法の遵守状況、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、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ことを追加している。また、共通化の考え方では、本人をだましての個人情報の取得は適正な取得とは言えないことなど、「偽りその他不正の手段」の具体例が示されている。

本WGでは、共通化の考え方を踏まえ、本ガイドライン第７条の「偽りその他不正の手段」について、解説で解釈を具体化するべきであるとの観点から議論を行い、具体例として、共通化の考え方で示された例に加え、さらに具体的な例を追加することが適当[1]との結論に至ったものである。

また、個人情報の適正な取得を目的とした第三者からの提供により個人情報を取得する場合については、共通化の考え方で示された望ましい事項に関し、本ガイドライン第７条の解説にわかりやすい形で記載を追加することが適当であると考えられる。

（２）改正内容

本ガイドライン第７条の解説において、「偽りその他不正の手段」の具体例として、以下の記載を追加することが適当であると考えられる。

① 本人をだましてその個人情報を取得する場合（虚偽の事業者名や利用目的を告げて個人情報を取得する場合や本人に対して個人情報を収集している事実を偽って個人情報を取得する場合など）

② 犯罪行為に該当する手段やプライバシー等の権利侵害となる手段により個人情報を取得する場合（他人が管理する個人情報を正当な権限なく取得す

[1] 具体的な例の追加に当たっては、園部逸夫編『個人情報保護法の解説《改訂版》』127 頁（ぎょうせい、2005）、宇賀克也『個人情報保護法の逐条解説［第４版］』87 頁（有斐閣、2013）、岡村久道『個人情報保護法〔新訂版〕』184 頁（商事法務、2009）における記述も参考としている。

る場合など）

③ 判断能力の乏しい子どもを通じて親の同意なしに親に関する個人情報を取得する場合

④ 偽りその他不正の手段により個人情報を取得した業者や第三者提供の制限に違反し個人情報を提供している業者から、事情を知って個人情報を取得する場合

また、第三者からの提供により個人情報を取得する場合には、提供元の法の遵守状況を確認し、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ことが望ましいこと、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、提供元における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ことを記載することが適当であると考えられる。

なお、共通化の考え方において、第三者からの提供により個人情報を取得する場合から除外されている場合[2]や、提供元の法の遵守状況の確認方法[3]についても具体的に記載することが適当であると考えられる。

２　第 11 条（安全管理措置）について

（１）検討の趣旨

共通化の考え方では、本情報漏えい事案を踏まえ、安全管理措置について、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に望ましい手法として、以下の例を追加している。

① 責任の所在の明確化のための措置

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

---

[2] 個人情報保護法第 23 条第１項各号に掲げる場合（第三者提供の制限の例外）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における個人情報の取得や、不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数の者により随時に購入することができるもの又はできたもの（個人情報保護法施行令第２条第２号）から個人情報を取得する場合

[3] 提供元の法の遵守状況としては、個人情報保護法第 23 条第２項又は第３項により本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしていることや、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することが考えられる。

③ 漏えい等に早期に対処するための体制整備
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
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
⑥ 盗難等の防止のための措置
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

上記①～⑦の例については、本ガイドラインの解説に追加することが適当であると考えられる。ただし、本ガイドラインでは、個人情報保護管理者に関する規定については別に第 13 条で規定しているため、上記①～⑦の内容のうち、個人情報保護管理者に係るものについては、同条の解説で記載することが適当であると考えられる。

（２）改正内容

本ガイドライン第 11 条の解説において、事業者の内部又は外部からの不正行為による個人情報の漏えい等を防止するために望ましい措置として、上記（１）①～⑦の例について（第 13 条に規定する個人情報保護管理者に係るものを除き）記載することが適当であると考えられる。ただし、本ガイドラインの解説では、安全管理措置について、技術的保護措置と組織的保護措置に分けて記載しているため、上記（１）①～⑦の例については、共通化の考え方そのままではなく、それぞれの措置ごとに整理をして、記載することが適当であると考えられる。

３　第 12 条（従業者及び委託先の監督）について

（１）検討の趣旨

共通化の考え方では、本情報漏えい事案を踏まえ、委託先の監督について、委託先における安全管理が図られるために望ましい手法として、以下の事項を追加している。

① 委託先の選定に当たっては、委託先の安全管理措置を確認し、適切に評価すること
② 委託契約等において、個人データを取り扱う者を明確にすることや再委託の際の手続き等を定めること
③ 委託先における個人データの取扱状況を調査するとともに、再委託先の安全管理措置を十分に確認すること

上記②の内容のうち契約内容が遵守されなかった場合の措置を定めること及び現行では本ガイドライン 12 条の解説で記載されている委託契約終了時の個人情報の取扱いについて、本ガイドライン第 12 条第４項に追加するとともに、①～③の内容については、同条の解説に追加することが適当であると考えられる。

また、従業者及び委託先の監督に当たっては、個人情報が漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、取り扱う個人情報の取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じることが求められることから、本ガイドライン第 12 条の解説にその旨を追加することが適当であると考えられる。

（２）改正の内容

本ガイドライン第 12 条第４項の本文に、委託契約において定めるべき事項として「委託契約終了時の個人情報の取扱い」、「契約内容が遵守されなかった場合の措置」を追加するとともに、同条の解説において、事業者の内部又は外部からの不正行為による個人情報の漏えい等を防止するために望ましい措置として、上記（１）①～③の内容を記載することが適当であると考えられる。

４　第 13 条（個人情報保護管理者）について

（１）検討の趣旨

共通化の考え方では、本情報漏えい事案を踏まえ、安全管理措置に関する望ましい手法として、責任の所在の明確化を挙げており、そのための手法の例として、個人情報保護管理者に、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ことを挙げている。また、内部規定や監査体制の整備に関しても、望ましい例を挙げている。

本ガイドラインにおいては、現行の第 13 条において、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、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、個人情報保護管理者を置いて、内部規程の策定、監査体制の整備等を行わせるものとすることを既に定めており、この第 13 条の規定に関連して、共通化の考え方で新たに盛り込まれた例等について、確認的に記載を追加することが適当であると考えられる。

（２）改正内容

本ガイドライン第 13 条の解説において、共通化の考え方を踏まえ、個人情報保護管理者となることが適当な者に関する記載や設置の意義に関する記載を追加するとともに、内部規程の策定や監査体制の整備において望ましい事項に関する記載を追加することが適当であると考えられる。

５　第23条（通信履歴）について

（１）検討の趣旨

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ことから、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、それらの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する必要がある。

この保存期間については、いかなる程度の期間が妥当であるかについて具体的な考え方が明示されておらず、電気通信事業者にとっての判断基準が不明確であるという指摘がある。

特に接続認証ログ[4]については、インターネット接続サービスにおいて、利用者からの問合せへの対応や、インターネット接続役務等の電気通信役務の安定的提供を図るためのマルウェア感染者への注意喚起や不正アクセス対策等のセキュリティ対策、適正な設備管理等における必要性が高く、消費者への適切な対応の確保やセキュリティ対策の向上、適正なネットワークの構築といった観点からは一定の期間の保存が必要となるものであるが、消費者保護の充実、セキュリティ対策の強化、通信の秘密やプライバシー保護等の要請を全体として勘案し、具体的にどの程度の期間の保存が適当かを判断することが事業者にとって難しい状況である[5]。

このため、通信履歴の保存期間に関し本ガイドラインにおいて一定の考え方を示した上で、特に、接続認証ログについては、その性質等を勘案し、一定の目的に関し一定の保存が認められる具体的な期間の目途を示すことが事業者により適切な判断を可能とする観点から適当と考えられるとともに、利用者にとっても事業者における保存の在り方についてより明確になるも

[4] 利用者を認証し、インターネット接続に必要となるＩＰアドレスを割り当てた記録。
[5] 実態としても、電気通信事業者ごとに保存期間は異なっている。

のと考えられる。

また、通信履歴の保存については、「サイバーセキュリティ戦略」等[6]で、サイバー犯罪に対する事後追跡可能性確保の観点からの検討も求められているが、本ガイドラインにおいて上記の改正を行うことは、この観点からの実質的な状況の進展にもつながるものであり、適切な方向性であると考えられる。

具体的には、接続認証ログについては、利用者からの契約や利用状況等に関する問合せ[7]やセキュリティ対策[8]への利用など業務上の必要性が高いと考えられる一方、利用者の表現行為やプライバシーへの関わりが、これらとの関わりがより直接的なウェブアクセスログ等と比較して小さいと考えられること[9]などを勘案し、正当業務行為として、一般に６か月程度の保存が認

---

6 ・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。

7 料金引落しにクレジットカードを利用するケースなどで利用から料金引落しまでに一定の期間を要し、実際の料金引落しの後、問合せ、苦情が生じる場合や、契約解約の有無に争いが生じ、利用状況の有無の確認をする必要がある場合など、実際の利用から問合せ、苦情等まで相当の時間がかかる場合を想定すると、６か月程度は対応可能な状態とすべきではないかと考えられる。

8 サイバー攻撃をする者が用意したＣ＆Ｃサーバ等に、マルウェアに感染しているコンピュータとの通信の記録（ＩＰアドレス等）が残っており、マルウェア感染端末の利用者に対し注意喚起をする場合があるところ、海外の攻撃者が用意したＣ＆Ｃサーバ等を海外の捜査機関等がテイクダウンした際等、捜査機関等から電気通信事業者に対する情報提供に長期間を要する場合が多い。また、悪意ある第三者等による不正侵入や不正操作等がなされた場合、その経緯を確認するため、相当前の接続認証ログを分析する場合もある。

9 接続認証ログがインターネットへの接続の記録であるのに対し、ウェブアクセスログは特定のウェブサイトへのアクセスの記録であり、接続認証ログと比較してウェブアクセスログは利用者の表現行為やプライバシーへの関わりが大きいため、より慎重な取扱いが求められると考えられる。

められると考えられ、また、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合[10]など、より長期の保存をする業務上の必要性がある場合には、事業者の判断により、例えば、１年程度保存することも正当業務行為として許容されると考えられ[11]、このような考え方を示すことが適当であると考えられる。

なお、正当業務行為として許容されるためには、漏えい等の防止についてセキュリティ上適切な対策が行われていることが求められることは言うまでもない。

また、法令の規定による場合その他特別の理由がある場合に例外的に保存し続けることができる場合についても、現行の法令についてより具体的に記載を追加することで明確化することが適当であると考えられる。

なお、本ガイドラインの今回の改正においては、正当な業務の遂行上の目的から認められうる保存期間を示すものであるが、今後、利用者利益の確保やセキュリティ対策の強化等を図る観点からは、同様のサービスを提供する各電気通信事業者の間において、保存期間についてある程度足並みを揃えていくことが有効であると考えられる。また、保存期間については、現状の利用状況や保存技術等を前提としたものであり、今後、利用状況や保存技術等の変化に伴い、変更されうるものと考えられる。

（２）改正内容

本ガイドライン第 23 条の解説の（５）以下の記述を以下のとおり（下線部が今回の改正による追加点）とすることが適当であると考えられる。

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（個人情報の本人が識別できなくすることを含む。）する必要がある。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。

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

10 年間の季節ごとの利用状況を把握することにより、適正なネットワークの構築を図ることができる場合がある。

11 利用者から通信履歴の保存期間等について問合せがあった場合、各電気通信事業者において、円滑なサービス提供への支障が生じるおそれがない場合には、当該通信履歴の保存期間及びその理由を説明することが望ましいと考えられる。なお、可能な場合には通信履歴の保存期間を公表することが望ましいとの指摘もあり、利用者への情報提供の在り方については、今後、必要な検討・取組を進めていくことが適当と考えられる。

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、業務の遂行上の必要性や保存を行った場合の影響等も勘案し、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。

例えば、通信履歴のうち、インターネット接続サービスにおける接続認証ログ（利用者を認証し、インターネット接続に必要となるＩＰアドレスを割り当てた記録）の保存については、利用者からの契約や利用状況等に関する問合せへの対応やセキュリティ対策への利用など業務上の必要性が高いと考えられる一方、利用者の表現行為やプライバシーへの関わりは比較的小さいと考えられることから、事業者がこれらの業務の遂行に必要とする場合、一般に６か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、１年程度保存することも許容されると考えられる。

ただし、刑事訴訟法第 197 条第３項及び第４項に基づく通信履歴の電磁的記録の保全要請[12]等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や特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成 13 年法律第 137 号）第４条に基づく発信者情報の開示請求の手続が開始された場合は、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。

〔６　第 26 条（位置情報）について〕

（１）検討の趣旨

本ガイドライン第 26 条第３項は、ＧＰＳ位置情報の捜査で利用する場合のルールを定めるものとして、平成 23 年の改正で盛り込まれたものであり、捜査機関が当該情報を取得するための要件として、裁判官の発付した令状に従うことのほか、「当該位置情報が取得されていることを利用者が知ることができるとき」との要件を課している。

この要件は、位置情報は、個々の通信に関係する場合は通信の秘密として保護され、個々の通信に関係しない場合であっても、ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が高いこと、また、各電気通信事業者が提供する位置情報通知サービスにおいては、「利用者の

12 情報処理の高度化等に対処するための刑法等の一部を改正する法律（平成 23 年法律第 74 号、平成 23 年６月 24 日公布、平成 24 年６月 22 日施行）により新設されたものである。

権利が不当に侵害されることを防止するため必要な措置を講ずる」ものとされており（本ガイドライン第 26 条第２項)、ＧＰＳ位置情報が取得される場合には画面表示や移動体端末の鳴動等がなされていること等を踏まえ、規定したものである。

しかしながら、本ガイドライン改正後も、犯罪捜査の場合においては、ＧＰＳ位置情報が取得されていることを被疑者等に知られてしまい、実効性のある捜査が困難となるため、捜査において活用することができない状況が生じている。また、通信の秘密の保護の対象である情報を捜査機関が利用する場合の手続（通信の傍受や通信履歴の利用など）と比較しても要件が過重でないかとの指摘もあり、本ガイドラインの改正についての検討が求められている[13]。

現行ガイドラインの「当該位置情報が取得されていることを利用者が知ることができるとき」という要件の趣旨は、ＧＰＳ位置情報が取得されていることを端末の画面上で表示する等の措置により、ＧＰＳ位置情報が常時取得されていることはないかといったプライバシー侵害に対する利用者の不安を払拭するためであると考えられる。

一方、当該要件により、刑事訴訟法上許容されている捜査手法について、ＧＰＳ位置情報が取得されていることを被疑者等に知られてしまい、実効性のある犯罪捜査が困難となり、適正かつ迅速な捜査がなされないということであれば、犯罪捜査の場合におけるＧＰＳ位置情報の取得に関する電気通信事業者の円滑な運用を確保する観点から規定された第 26 条第３項の趣旨を達成できないという課題がある。

犯罪捜査の場合においては、電気通信事業者がＧＰＳ位置情報を取得するためには、裁判官の発付した令状に従う必要があり、司法手続が適正になされている限り、利用者のプライバシー等に対する配慮が十分になされているといえる。

したがって、本ガイドライン第 26 条第３項の「当該位置情報が取得され

13 ・前掲「「世界一安全な日本」創造戦略」
携帯電話のＧＰＳ位置情報に係る捜査の実効性の確保
振り込め詐欺等の被疑者の所在地等の特定のための携帯電話端末のＧＰＳ位置情報の取得について、関係ガイドラインの見直しを含め、捜査の実効性が確保されるような仕組みの構築に向けて検討する。

ていることを利用者が知ることができるとき」という要件は、削除することが適当であると考えられる。

（２）改正内容

本ガイドライン第 26 条第３項の「当該位置情報が取得されていることを利用者が知ることができるときであって、」及び同解説の「位置情報の取得について、画面表示や移動体端末の鳴動等の方法により、当該位置情報が取得されていることを利用者が知ることができるときであって、かつ、」を削除することが適当であると考えられる。