財団法人 日本データ通信協会
Japan Data Communications Association

電気通信事業における
個人情報保護指針

平成２２年１１月

認定個人情報保護団体

財団法人日本データ通信協会

≪ 目 次 ≫

P. 1 はじめに
P. 3 第1章 法及びガイドラインの遵守等
P. 3 1. 定義（ガイドライン第2条）
P. 5 2. 法及びガイドラインの遵守（ガイドライン第3条第1項）
P. 6 3. 通信の秘密に属する事項について留意すべき事項（ガイドライン第3条第2項、第3項）
P. 8 第2章 個人情報の適正な取扱いの確保
P. 9 1. 取得の制限（ガイドライン第4条）
P. 11 2. 利用目的の特定（ガイドライン第5条）
P. 17 3. 利用目的による制限（ガイドライン第6条）
P. 19 4. 適正な取得等（ガイドライン第7条）
P. 20 5. 取得に際しての利用目的の通知等（ガイドライン第8条）
P. 25 6. 正確性の確保（ガイドライン第9条）
P. 26 7. 保存期間等（ガイドライン第10条）
P. 30 8. 安全管理措置（ガイドライン第11条）
P. 46 9. 従業者及び委託先の監督（ガイドライン第12条）
P. 55 10. 個人情報保護管理者（ガイドライン第13条）
P. 56 11. プライバシーポリシー（ガイドライン第14条）
P. 60 12. 第三者提供の制限（ガイドライン第15条）
P. 70 13. 個人情報に関する事項の公表等（ガイドライン第16条）
P. 73 14. 個人情報の開示及び訂正等（ガイドライン第17条）
P. 77 15. 理由の説明（ガイドライン第18条）
P. 78 16. 開示等の求めに応じる手続（ガイドライン第19条）
P. 90 17. 手数料（ガイドライン第20条）
P. 92 18. 苦情の処理（ガイドライン第21条）
P. 99 19. 漏えい等が発生した場合の対応（ガイドライン第22条）
P.110 20. 各種情報の取扱い
P.111 第3章 指導、勧告その他の措置（法第43条）
P.112 第4章 指針の見直し

別紙
P.113 事故報告書

参考資料1

P.115　例　1　個人情報の利用目的の一部変更のお知らせ（例）
P.116　例　2　就業時の秘密保持誓約書（例）
P.119　例　3　退職時の秘密保持誓約書（例）
P.121　例　4　個人情報保護に関する委託先との覚書（例）
P.127　例　5　プライバシーポリシー（例）
P.132　例　6　個人情報の利用目的通知申請書（例）
P.133　例　7　個人情報の利用目的の回答書（例）
P.134　例　8　個人情報の開示申請書（例）
P.135　例　9　個人情報の開示についてのお知らせ（例）
P.136　例10　個人情報の開示及び一部非開示についてのお知らせ（例）
P.137　例11　個人情報の非開示についてのお知らせ（例）
P.138　例12　個人情報の訂正・追加・削除申請書（例）
P.139　例13　個人情報の利用停止・消去申請書（例）
P.140　例14　個人情報の第三者提供停止申請書（例）
P.141　例15　個人情報の訂正等措置回答書（例）
P.142　例16　委任状（例）

参考資料2

P.143　ノートブック型パーソナルコンピュータ等の社外への持出しにおける適切な技術的保護措置について

参考資料3

P.165

参考資料3－1

総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言（平成22年5月）の抜粋

Ⅱ　ライフログ活用サービスに関する検討について

5. より信頼されるサービスに向けて（配慮原則の提言）

参考資料3－2

総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言（平成22年5月）の抜粋

Ⅲ　安全管理措置に関する検討について

2. 想定されるリスクと技術的対応策

3. 求められる安全管理措置

改 正 履 歴

項番	改正年月日	主な改正内容等
1	平成17年4月	（新規作成）
2	平成18年12月12日	「漏えい等が発生した場合の対応」について、留意点等の内容を補強した。
3	平成19年9月12日	社員情報については、雇用管理に関する個人情報と考えられ、厚生労働省の指針の対象にもなっていることに留意する必要があることを補強した。
4	平成22年3月29日	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及び解説の改正（消費者等の権利利益の一層の保護に関する事項ほか）に伴う改正及び全面的な見直し。
5	平成22年11月17日	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及び解説の改正（匿名化を行うことは利用目的として特定する必要はない、モバイルPC等による個人情報の持出時に求められる安全管理措置の在り方ほか）に伴う改正ほか。

電気通信事業における個人情報保護指針

平成１７年４月
財団法人日本データ通信協会
電気通信個人情報保護推進センター
（最終改正：平成２２年１１月１７日）

はじめに

平成１７年４月１日に個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）が全面施行されたのを受けて、財団法人日本データ通信協会は、電気通信事業者の個人情報の適正な取扱いの確保を目的として、電気通信事業者の個人情報の取扱いに関する苦情の処理、個人情報の適正な取扱いの確保に寄与する事項についての電気通信事業者に対する情報の提供等の業務を行うこととし、平成１７年４月１２日、法第３７条第１項に基づき認定個人情報保護団体として、総務大臣及び経済産業大臣の認定を受けた。

認定個人情報保護団体は、個人情報の適正な取扱いの確保に寄与する事項についての電気通信事業者に対する情報の提供を行うことを業務としており、その情報提供の一つの形態として、個人情報保護指針を作成し公表していくことが個人情報の適正な取扱いの確保に有効と考えられることを踏まえ、法は、認定個人情報保護団体に対して個人情報保護指針を作成し公表するよう努めることを求めている。

本指針は、認定個人情報保護団体たる当協会が、法第４３条に基づいて、電気通信事業者の個人情報の適正な取扱いの確保のために、利用目的の特定、安全管理のための措置、本人の求めに応じる手続等に関し、法及び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。以下「ガイドライン」という。）及びその解説（以下「解説」という。）の趣旨に沿ったものとして、作成し公表するものである。

電気通信事業分野においては、法第６条及び第８条に基づき、電気通信事業法第４条その他の規定の趣旨を踏まえ、すでに平成１６年８月にガイドラインが告示されているところである。本指針は、電気通信事業者がガイドラインを適切に遵守できるよう、ガイドラインにおける利用目的の特定、安全管理のための措置、本人の求めに応じる手続等の規定に関して、それぞれ好ましい事例、好ましくない事例、業務フローチャート、及び参考となる書式例等を示すなど個人情報の取扱いについての実務上の手引きとして作成したものであり、もって個人情報の特に適正な取扱いの厳格な実施を確保する必要がある電気通信事

業分野全体の個人情報保護の水準の向上に資することを目的としている。
　法は、認定個人情報保護団体に対して、対象事業者に個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとるよう努めることを求めており、対象事業者は、当然、この指針を守らなければならない。また、対象事業者となっていない電気通信事業者であっても、法及びガイドラインに基づく対応をするにあたり、この指針を参考にしていただきたい。

［凡例］

（表記）	（正式名称）
法	個人情報の保護に関する法律（平成１５年法律第５７号）
ガイドライン	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）
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）の解説

（注）実線の枠内には、法及びガイドラインの条文又は解説を引用し、その下に趣旨や留意点等を説明している。また、好ましい事例及び好ましくない事例は破線の枠内に記述した。

第１章　法及びガイドラインの遵守等

１．定義（ガイドライン第２条）

［ガイドライン］

第2条　このガイドラインにおいて使用する用語は、個人情報の保護に関する法律（平成15年法律第57号）第2条において使用する用語の例によるほか、次の定義に従うものとする。

一　電気通信事業者　電気通信事業（電気通信事業法（昭和59年法律第86号）第2条第4号に定める電気通信事業をいう。）を行う者をいう。

二　電気通信サービス　電気通信事業者が業務として提供する電気通信役務（電気通信事業法第2条第3号に定める電気通信役務をいう。）及びこれに付随するサービスをいう。

三　利用者　電気通信サービスを利用する者をいう。

四　加入者　電気通信事業者との間で電気通信サービスの提供を受ける契約を締結する者をいう。

（第2条の解説）

(1) 本ガイドラインで使用する基本的用語を定めるものであるが、電気通信事業を行う者が取り扱う個人情報を広く対象とするため、電気通信事業法の用例とは必ずしも一致しない。

(2)「電気通信事業者」とは、電気通信事業法上は、電気通信事業を営むことについて、登録、届出という行政上の手続を経た者をいうが、同じサービスを提供しながら本来行わなければならない手続を経ていないという理由でガイドラインの対象外となるのは不合理であるので、本ガイドラインでは、こうした手続の有無にかかわらず、電気通信事業を営む者を対象とすることとした。なお、電気通信事業法の適用除外とされている同法第164条第1項各号に定める事業を営む者についても、同法第4条（秘密の保護）の規定の適用があり個人情報保護の必要性に差はないことから、本ガイドラインの対象とすることとした。また、営利を目的とせずに電気通信事業を行う者についても、個人情報を適正に取り扱うことは求められることから、本ガイドラインの対象とすることとした。

(3) 電気通信事業者の事業の中心は、電気通信役務（電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の用に供すること。）を他人の需要に応じて提供することであるが、それ以外にもこれに付随するサービスを行っており（電話帳発行業務等はこれに当たる。）、これらの業務の過程において取り扱う利用者の個人情報についても適正な取扱いが要請されることから、これらを含めたものを「電気通信サービス」とし、ガイドラインの対象とすることとした。

(4)「利用者」とは、電気通信事業法上は、電気通信事業者との間に電気通信役務の提供を受ける契約を締結する者をいうが、加入電話にみられるように契約者でなくとも電気通信サービスの利用は可能であることから、これらの者の個人情報をも保護するため、単なる電気通信サービスの利用者を「利用者」としてガイドラインの対象とすることとした。

(5)「加入者」とは、電気通信事業法上の「利用者」に該当する者をいう。

(6) 第１号から第4号に規定する用語以外で、このガイドラインにおいて使用する用語は、個人情報保護法第2条において使用する用語の例によることになる。

なお、個人情報保護法第2条第1項においては、「個人情報」とは「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。」と定義されている。

このうち、「個人」とは、日本国民に限られず、外国人も含まれる。また、公務員及び公人も「個人」に当たる。法人その他の団体は「個人」に該当しないため、法人その他の団体に関する情報は個人情報に含まれない。ただし、法人その他の役員に関する情報は個人情報に当たる。

「個人に関する情報」とは、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、社会的地位、身分等の属性に関して、事実、判断、評価を表すすべての情報をいい、評価情報といわれるものも含まれる上、公刊物等によって公にされているものも含まれる。

「その他の記述等」とは、氏名、生年月日以外の記述又は個人別に付された番号、記号その他の符号等をいう。映像、音声もそれによって個人の識別に至る限りは「等」に含まれる。

(7) 本ガイドラインは、個人の権利利益の保護を目的とすることから、個人を識別することができない情報は除く一方、他の情報と照合することによって個人を識別することができる場合は対象としている。もっとも、他の情報との照合が容易でない場合については、個人の識別が容易ではなく、個人の権利利益を侵害するおそれも小さいと認められることから、個人情報の範囲から除外している。具体的には、他の電気通信事業者への照会を要する場合のほか、内部でも取扱部門が異なる等の事情により照会が困難な場合がこれに当たる。

なお、本ガイドラインでは、死者に関する情報は、死者と生存する者の双方に関する情報を除き、対象としていないが、死者に関する情報についても適正に取り扱う必要があることは生存する者に関する情報と同様であり、死者に関する情報についても、安全管理措置の実施等基本的には生存する者に関する情報と同様に本ガイドラインに定める措置をとり適正に取り扱うことが求められる。また、電気通信事業法の通信の秘密の保護の対象は、生存する者に限定されていないことにも留意する必要がある。

本指針において使用する用語は、法及びガイドラインにおいて使用する用語の例による。

２．法及びガイドラインの遵守（ガイドライン第３条第１項）

[ガイドライン]
第3条　本ガイドラインの規定は、個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めるものとして、解釈され、運用されるものとする。

（第3条第1項の解説）
(1) 本ガイドラインは、電気通信事業者に対する個人情報保護法の適用の基準を明らかにするとともに、通信の秘密に係る電気通信事業法第4条その他の関連規定を踏まえ、特に個人情報の適正な取扱いの厳格な実施を求められる電気通信事業者が、個人情報の取扱いに当たり遵守すべき基本的事項を明らかにするものである（第1項）。

電気通信事業者は、法、通信の秘密に係る電気通信事業法の規定その他の関連法令及びガイドラインの規定を遵守しなければならない。

３．通信の秘密に属する事項について留意すべき事項（ガイドライン第３条第２項、第３項）

３－１．法人の情報も保護の対象

[ガイドライン　第3条]

第2項　電気通信事業者は、個人情報の保護に関する法律の規定及び通信の秘密に係る電気通信事業法第4条その他の関連規定を遵守するほか、このガイドラインに従い個人情報を適正に取り扱うものとする。

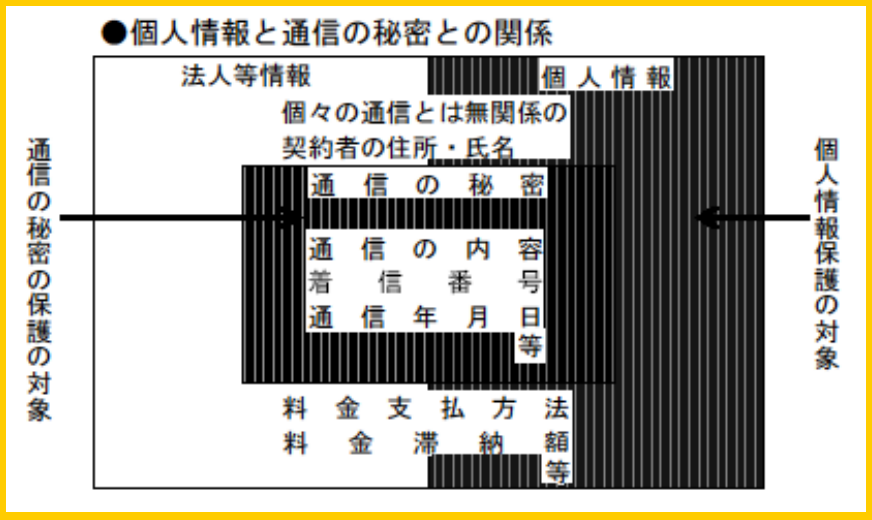
第3項　電気通信事業者は、第3章に規定する各種情報については、第2章に規定する個人情報の取扱いに関する共通原則を遵守するほか、第3章の規定に従い適正に取り扱うものとする。

（第3条第2項、第3項の解説）

⑵　第2項は、個人情報の取扱いに関し、個人情報保護法の規定及び通信の秘密に係る電気通信事業法第4条その他の関連規定と本ガイドラインの規定の適用関係を明確にするものである。

上記⑴で述べたとおり、本ガイドラインは、電気通信事業者に対する個人情報保護法の適用の基準を明らかにするものであるので、電気通信事業者は、本ガイドラインの規定を遵守すれば電気通信事業に関しては個人情報保護法の規定は遵守したこととなる。

一方、通信の秘密に係る電気通信事業法第4条その他の関連規定については、通信の秘密に属する事項については、個人の情報であるか、法人その他の団体の情報であるかの区別なく保護されるものであることから、法人その他の団体に関するものも保護の対象となる（下記図参照）など、その対象及び規律の内容について、本ガイドラインの範囲を超える場合がある。



⑶　第3項は、第3章に規定する各種情報の取扱いに関し、同章の規定と第2章の規定の適用関係を明確にするものである。第3章の規定は、同章に規定する各種情報について、第2章の共通原則に対する特則的な規定であり、第3章に規定する各種情報についても、同章に特に規定されていない事項については、第2章の共通原則によるべきものである。

通信の秘密に属する事項については、個人の情報であるか、法人その他の団体の情報であるかの区別なく保護されるものであり、電気通信事業者においては、通信の秘密に属する情報を取り扱うにあたっては、特に注意することが必要である。

３－２．安全管理措置や従業者の研修等における配慮

通信の秘密に属する情報については特に厳重な安全管理措置を講ずるとともに、通信の秘密の保護については従業者の研修においても個人情報保護とは項目を分けて説明するなど、通信の秘密に属する情報の取扱いには万全を期するよう配慮することが必要である。

第２章　個人情報の適正な取扱いの確保

本章においては、ガイドラインに規定する事項のうち、個人情報の適正な取扱いの確保のために特に注意を要すると思われるものを取り上げて、解説し、実務上の参考となるよう適宜好ましい事例及び好ましくない事例を可能な限り取り入れた。ここで好ましい事例とは、電気通信事業者がこれに従っていれば法及びガイドラインに違反することにはならないものであるが、もちろん、ここで列挙した事例以外にも法及びガイドラインに違反しない場合はあり得るものである。また、好ましくない事例とは、電気通信事業者が、これに該当している場合には法やガイドラインの規定に違反することとなるものであり、厳に避けるべきものである。

１．取得の制限（ガイドライン第４条）

１－１．制限

［ガイドライン］
第４条　電気通信事業者は、電気通信サービスを提供するため必要な場合に限り、個人情報を取得するものとする。

（第４条第１項の解説）
(1) 第１項は、電気通信事業者が個人情報を取得できる場合を電気通信サービスの提供上必要な場合に限ることにより、不必要な個人情報の取得を防ぐこととするものである。ただし、「電気通信サービスを提供するため必要な場合」には、現在提供している電気通信サービスのために直接必要な場合に限らず、それと関連性を有する場合（例えば、新サービス提供のためのアンケート調査を行う場合等）も含まれる。

電気通信事業者が個人情報を取得できる場合を電気通信サービスの提供上必要な場合に限ることにより、不必要な個人情報の取得を防ぐこととするものである。

○（好ましい事例）

事例１－１　電気通信サービスを提供するにあたって必要となる個人情報が氏名、住所、電話番号、クレジットカード番号である場合に、これらの情報のみを取得する。

×（好ましくない事例）

事例１－２　個人向けインターネット接続サービスを提供するにあたって必要がないにもかかわらず勤務先情報を取得し、本人が銀行振込での支払いを希望しているにもかかわらずクレジットカード番号を取得する。

１－２．センシティブとされる個人情報

[ガイドライン第４条]
第２項　電気通信事業者は、次の各号に掲げる個人情報を取得しないものとする。ただし、自己又は第三者の権利を保護するために必要な場合その他社会的に相当と認められる場合はこの限りでない。
一　思想、信条及び宗教に関する事項
二　人種、門地、身体・精神障害、犯罪歴、病歴その他の社会的差別の原因となるおそれのある事項

（第４条第２項の解説）
(2) 第２項は、センシティブとされる個人情報（思想、信条及び宗教に関する個人情報や社会的差別の原因となるおそれのある社会的身分に関する個人情報）については、原則として取得を禁止することとするものである。しかし、例えば、移動体通信事業者が契約締結の際に本人確認のため提示を要求する免許証や健康保険証にはセンシティブな情報が含まれることがあり、また、宅内機器の割引使用料を適用するために利用者が身体障害者である旨の情報を得ることもある。加入者の使用言語などの情報も場合によれば社会的差別の原因となる事項といえるが、国際通信事業者等がそのサービス向上のためにこれを取得することは可能というべきであろう。さらに、電気通信事業者が加入者と紛争関係に立った場合に自己の権利を守るためにその者に関する個人情報を広く取得する必要がある場合もある。したがって、これら社会的に相当と認められる場合には例外を認めることとした。なお、この場合においても、こうした情報に基づいて、電気通信事業者が不当な差別的取扱いをすることは許されず、電気通信事業法上も同趣旨の規定がある（同法第６条及び第２９条第１項第２号）。

センシティブとされる個人情報（思想、信条及び宗教に関する個人情報や社会的差別の原因となるおそれのある社会的身分に関する個人情報）については、原則として取得を禁止することとするものである。

×（好ましくない事例）

事例１－３　電気通信サービスを提供するにあたって必要となる個人情報が氏名、住所、電話番号、クレジットカード番号だけであるにもかかわらず必要のないセンシティブな本籍情報を取得する。

事例１－４　電気通信サービス契約時の審査や契約変更申込時の本人確認資料として提供を受けた運転免許証や健康保険被保険者証から、必要のない臓器提供の希望の有無の情報を取得する。

２．利用目的の特定（ガイドライン第５条）

２－１．利用目的の特定

[ガイドライン]

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。

（第５条の解説）

(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。

(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。

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する必要はない。

利用目的の特定にあたっては、利用目的を抽象的に特定するのではなく、可能な限り具体的に特定する必要がある。利用目的の特定にあたっては、業務ごとに取り扱う個人情報の項目を列挙し、どのような業務でどのような個人情報が取り扱われるのか加入者が理解できるよう分かりやすく記載することが適当である。

なお、匿名化を行って個人識別性を完全に喪失させる行為は、個人情報の利用に当たらず、電気通信事業者は利用目的として特定する必要はない。

＜匿名化の例＞

- アンケートで取得した個人情報のうち、氏名や住所等の個人を識別し得る部分を完全に抹消し、性別、年齢等の属性情報を統計データとして蓄積し、新サービスの企画、開発に活用する。
- 新しい情報システムのテストデータを作成するために、顧客マスタファイルから、個人を識別し得る部分をダミーデータに置き換え、元データとダミーデータの対応表を保有しない。

≪参考≫

個人の生活の履歴であるライフログを活用したサービスについては、必ずしも個人を識別する必要がないため、そもそも個人を識別しない形態で情報を取得したり、保有する個人情報に匿名化を行うことで個人識別性を喪失させたりして、個人に関する情報の利活用を容易にする取組がなされている。

個人識別性を喪失した情報には個人情報保護法及び関係各ガイドラインの保護が及ばないほか、匿名化という行為自体も利用目的として特定する必要がないものの、ライフログを活用するサービスは、その態様によっては、プライバシーを侵害し得るし、利用者の不安感等を惹起し得る。よって、ライフログを取得・保存・利活用する事業者は、利用者に対して一定の配慮をなし、円滑なサービスに資するための対策を取ることが望ましい。

なお、ライフログ活用サービスの現状や問題点、配慮原則等については、総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」で検討され第二次提言として公表されている。（平成22年5月）

具体的な「配慮原則」については、参考資料3－1 総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言の抜粋（注）を参照されたい。

（注）参考資料3－1は総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言から次の部分を抜粋している。

Ⅱ　ライフログ活用サービスに関する検討について

5. より信頼されるサービスに向けて（配慮原則の提言）

○（好ましい事例）

事例２－１　各業務に必要となる個人情報を具体的に明示している。

（例）当社は、電気通信サービスの提供にあたって行う次の業務のために、それぞれ次のお客様の個人情報を利用します。

・料金計算及び請求業務

氏名、住所、電話番号、料金請求に必要となる金融機関の口座番号及び名義、クレジットカード番号、お申し込みのサービス内容

・お客様相談対応業務

氏名、住所、電話番号、メールアドレス、お申し込みのサービス内容

・新サービスに関する情報提供業務

氏名、住所、電話番号、メールアドレス

×（好ましくない事例）

事例２－２　「当社は、当社の事業運営のためにお客様の個人情報を利用します。」のように利用目的が具体的に特定されておらず、また、利用する個人情報を明確にしていない。

事例２－３　電気通信サービスを提供するにあたって利用することとなる個人情報が具体

的に記載されていない。

（例）当社は、お客様の個人情報を電気通信サービス提供のために利用します。

２－２．利用目的の変更

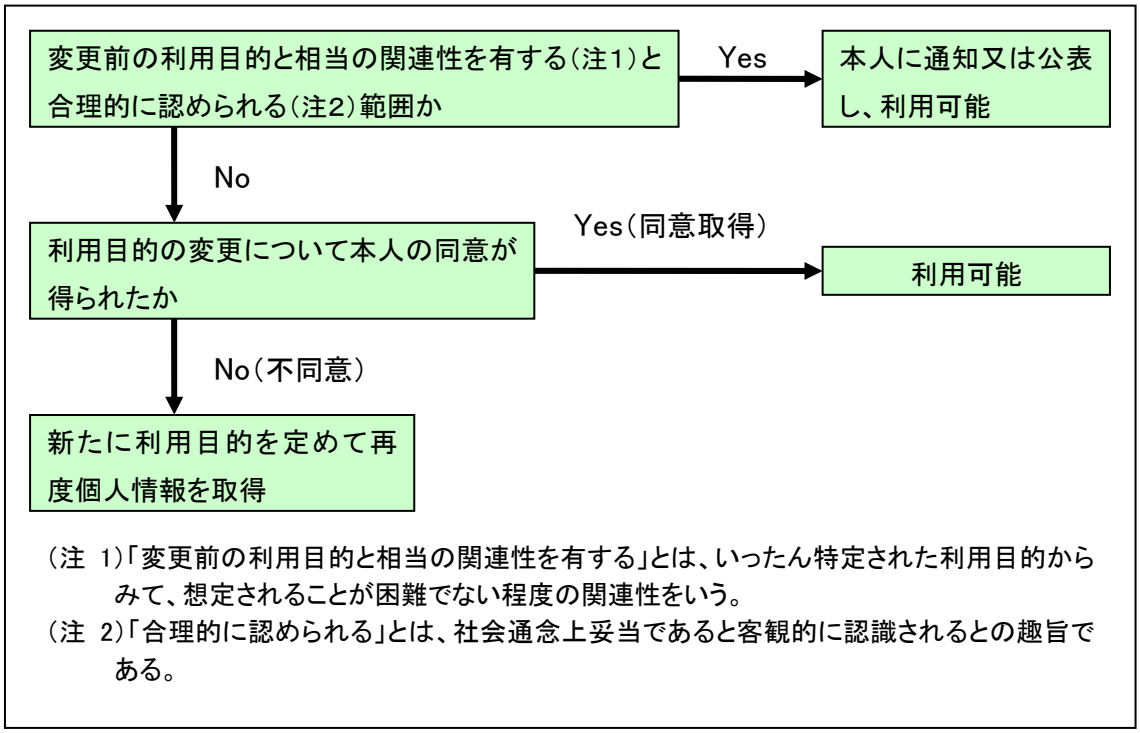
［ガイドライン第５条］
第２項　電気通信事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行わないものとする。

（第５条第２項の解説）
⑶　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。
「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。

原則として利用目的は変更しないことが望ましいが、一旦特定した利用目的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において変更することも許されないわけではない。その場合においても本人に通知するか、公表しなければならない。（ガイドライン第８条第３項参照。）

利用目的の変更が、変更の許容範囲を超えることとなる場合には、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。

《参考》利用目的の変更のフロー



（注 1）「変更前の利用目的と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いう。

（注 2）「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。

○（好ましい事例）

事例２－４　「当社の新サービスの案内の電子メールの送付」に利用することを利用目的として取得した契約者の個人情報を、「ＤＭによる新サービスの案内」に利用するにあたり、利用目的の変更及びＤＭ送付の停止依頼を受け付けることを電子メールで本人に通知した。

事例２－５　「アンケート集計に利用」することを利用目的として取得した個人情報を、「当社サービスのＤＭの郵送」に利用することは、本人が想定できる範囲を超えた利用目的の変更と考えられたため、改めて「当社サービスのＤＭの郵送」に利用することについての本人の同意を得た。

×（好ましくない事例）

事例２－６　当初の利用目的が「当社は、アンケートにより取得したお客様の氏名、住所、電話番号については、ＩＰ電話サービスの新サービスのご案内において使用します。」となっていたものを、「当社は、アンケートにより取得したお客様の氏名、住所、電話番号については、ＩＰ電話サービスの新サービス及び当社と提携している○×会社の各種商品案内に使用します。」へお客様の同意を得ずに変更する。

２－３．利用目的の範囲

［ガイドライン第５条］
第３項　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。

（第５条第３項の解説）
(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．利用目的による制限（ガイドライン第６条）

[ガイドライン]

第6条　電気通信事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱わないものとする。

第2項　電気通信事業者は、合併その他の事由により他の電気通信事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱わないものとする。

第3項　前2項の規定は、次に掲げる場合については、適用しない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

第4項　前項の規定にかかわらず、電気通信事業者は、同項各号に掲げる場合であっても、利用者の同意がある場合その他の違法性阻却事由がある場合を除いては、前条の規定により特定された利用目的の達成の範囲を超えて、通信の秘密に係る個人情報を取り扱わないものとする。

（第6条の解説）

(1) 本条は、電気通信事業者に対して、個人情報の取扱いを利用目的の達成に必要な範囲内に限ることにより、無限定な個人情報の取扱いを排除することを通じて、本人の権利利益侵害を防止しようとするものである。

「個人情報の取扱い」とは、個人情報に関する一切の行為を含む概念であることから、何が「必要な範囲」かについては、様々な側面からこれを判断する必要がある。すなわち、個人情報の取扱いの手段、方法はもちろん、取り扱う個人情報の内容、量等についても、必要な限度を超えないことが必要である。したがって、利用目的に照らして過剰な個人情報の取得も本条によって規制されることになる。例えば、加入者の本人確認のために、加入者の収入や学歴等は必要とはいえず、取得は制限される。

(2) 合併や営業譲渡などにより事業の承継があった場合、通常その承継資産には顧客情報等の個人情報が含まれると考えられ、必然的に個人情報が移転する。この場合において、事業を承継した電気通信事業者が自由に利用目的を設定することとなれば、本人にとって不測の権利利益の侵害が生じるおそれが高まることとなる。このため、合併その他の事由により他の電気

通信事業者から事業を承継することに伴って個人情報を取得した場合には、事業承継後においても、本人の同意なく当該個人情報に係る承継前の利用目的の達成に必要な範囲を超えて取り扱ってはならないこととする。

(3) 電気通信事業者が取得した個人情報については、電気通信サービスの円滑な提供のため、又は本人の利益や社会公共の利益のために目的外利用が要請される場合もあるので、そうした場合を目的外利用の禁止の例外として第3項各号に定めている。

なお、同項各号に該当する場合の本人の同意なき個人情報の目的外利用については、個人情報保護の要請が特に高い電気通信事業者としては、本人の同意を得ずに目的外利用を行うことが真に必要であると慎重に判断した上で行うこととすべきである。

なお、本項各号の規定により目的外で利用する必要性がある場合の多くは、個人情報を第三者に提供する必要性がある場合と想定されることから、第１項の「本人の同意」の趣旨及び本項各号の規定内容の趣旨については、第15条の解説を参照されたい。

(4) 第4項の規定は、第3項各号の規定の適用がある場合であっても、個人情報が通信の秘密にも該当する場合には、通信当事者の同意なき利用は、違法性阻却理由がある場合を除き許されないことについて念のため確認する趣旨の規定である。

電気通信事業者が契約の際に取得した個人情報を別のサービスの案内に利用する場合、次のような点に注意する必要がある。

- 個人情報の利用目的として他のサービスの案内に利用することを定めることは可能であるが、契約の時点でその利用目的を定めていなかった場合には、他のサービスの案内に利用することについて本人の同意を得る必要があること。
- 電気通信事業者は、本人との間で契約を結ぶことに伴って、契約書などの書面で個人情報を取得する場合には、あらかじめ本人に対してその利用目的を明示することとされている。（ガイドライン第８条第２項）契約の際に取得した個人情報を他のサービスの案内に利用すること自体は可能であるが、その場合には、電気通信事業者は、個人情報の取得前に、本人に対してその旨を明確に示すことが必要であること。

４．適正な取得等（ガイドラン第７条）

[ガイドライン]
（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。

（第7条の解説）
　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ず、偽りその他不正の手段によることは許されない。

　電気通信事業者は、偽り等の不正の手段により個人情報を取得してはならない。

〇（好ましい事例）

事例４－１　加入申込を受け付ける際やアンケートを実施する際に、利用目的を明示して、本人から同意を得て個人情報を取得する。

×（好ましくない事例）

事例４－２　関連会社間で顔なじみの社員同士が勝手にお客様名簿を交換しあう。

５．取得に際しての利用目的の通知等（ガイドライン第８条）

５－１．利用目的の通知・公表

[ガイドライン]
第8条　電気通信事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表するものとする。

（第8条の解説）
(1) 本条は、電気通信事業者に対して、利用目的を通知・公表させることにより、本人の不安感を緩和するとともに、本人自らが必要な注意を払うための契機を提供することにより、本人の権利利益侵害を予防しようとするものである。
(2)「通知」とは、例えば、郵便、電話、電子メール等によって利用目的を知らせることが想定される。「公表」とは、例えば、インターネット上での公表、パンフレットの配布、事業所の窓口等への書面の掲示・備付け等が想定される。

① 「本人に通知」とは、本人に直接知らしめることをいい、利用目的が本人に認識される合理的かつ適切な方法によらなければならない。

○（好ましい事例）

事例５－１　個人情報の取得に際して、次のようにして本人へ利用目的を通知する。
・利用目的を記載した文書を手交して口頭で説明する。
・利用目的を記載した文書を電子メール、ファックス等により送信し、又は郵送する。

② 「公表」とは、広く一般に自己の意思を知らせること（国民一般その他不特定多数の人々が知ることができるように発表すること）をいう。ただし、公表にあたっては、利用目的が本人に認識される合理的かつ適切な方法によらなければならない。

○（好ましい事例）

事例５－２　利用目的を、自社のホームページへの掲載、自社の店舗及び事務所内においてポスター等の掲示、パンフレット等の備え置き及び配布するなどして公表する。

③個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

（例）

- 電話帳や職員録等から個人情報を取得した場合
- 個人情報の第三者提供を受けて、個人情報を取得した場合
- 個人情報の取扱いの委託を受けて、個人情報を取得した場合

○（好ましい事例）

事例５－３　Ａ通信会社は、Ｂ通信会社に回線工事の一部を委託し、関係する契約者の個人情報をＢ通信会社に提供している。Ａ通信会社は、契約者情報を回線工事のために利用すること及び回線工事を委託することに関する事項をプライバシーポリシーに記載し公表している。Ｂ通信会社は、そのプライバシーポリシーにおいて、受託している業務に関して取得した個人情報は、当該受託業務のためにのみ利用することを公表し、受託した回線工事の業務だけに当該個人情報を使っている。

５－２．本人に対しその利用目的を明示

[ガイドライン第8条]
第2項　電気通信事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

（第8条第2項の解説）
(3) 第2項は、契約や調査等のため、書面やコンピュータを用いて直接本人から個人情報を取得する場合には、個人情報を取得した後に利用目的を通知・公表することで足りることとはせず、原則として取得前に本人に対して利用目的を明示するものとすることとするものである。明示の方法としては、契約締結時に契約内容を説明する書面に利用目的を記載し、それを契約締結前に交付して示すことなどが想定される。
　同項ただし書は、人の生命、身体又は財産の保護のために緊急に必要がある場合にまで、あらかじめその利用目的を明示するものとすることは合理性に欠けることから、このような場合には、取得前の明示は免除するものである。なお、このような場合には、第１項の規定に従って、取得後速やかにその利用目的を通知・公表するものとすることとなる。

「本人に対し、その利用目的を明示」とは、本人に対し、その利用目的を明確に示すことをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

○（好ましい事例）

事例５－４　電気通信サービスへの新規契約を受け付ける際に、契約書などに利用目的を明示し、本人に手渡す。利用目的は本人の目にとまりやすい場所に記載する等、本人が実際に利用目的を目にできるよう留意する。

事例５－５　ネットワーク上において個人情報を送信する前にその利用目的が本人の目に留まるよう配慮した配置とする。（同じページに利用目的が記載できない場合でも１回程度の操作で参照できるようにリンクやボタンを設定する。）

５－３．利用目的の変更の通知・公表

[ガイドライン第8条]
第3項 電気通信事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表するものとする。

（第8条第3項の解説）
(4) 第3項は、利用目的を変更した場合にも通知・公表する必要があることを確認的に規定しているものである。なお、この場合の「利用目的の変更」は、第5条第2項に規定する「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」内で行わなければならないことは当然である。

電気通信事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表する必要がある。また、利用目的を変更する場合には、次の点を留意されたい。

- ホームページ等に公表している利用目的については、その利用目的の制定日を付記することが望ましいこと。
- これを変更した場合、変更年月日、変更点等も併せて、公表するか又は問合わせに直ちに応えられるようにしておくことが望ましいこと。
- 利用目的の変更の記録は少なくとも取得個人情報を保存している間は、保持することが望ましいこと。

利用目的変更についての通知・公表の記載例を参考資料１の例１に示す。これは、電気通信事業者が利用目的の一部変更の通知・公表を行うにあたっての参考として示すものである。

○（好ましい事例）

事例５－６　グループ会社と契約者情報を共同利用することを利用目的に追加した。既存契約者全員に利用目的変更についての同意書を送付し、同意を得た契約者の情報だけを共同利用した。

５－４．利用目的の通知・公表等の適用除外

［ガイドライン第8条］

第4項 前3項の規定は、次に掲げる場合については、適用しない。

一 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二 利用目的を本人に通知し、又は公表することにより当該電気通信事業者の権利又は正当な利益を害するおそれがある場合

三 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

四 取得の状況からみて利用目的が明らかであると認められる場合。

６．正確性の確保（ガイドライン第９条）

[ガイドライン]
第9条　電気通信事業者は、利用目的の達成に必要な範囲内において、個人情報を正確かつ最新の内容に保つよう努めるものとする。

（第9条の解説）
(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、個人情報の正確性の確保に努めるものとすることを規定したものである。
(2) 誤った個人情報、現行化されていない個人情報が利用・提供されたときは、その個人の権利利益が侵害されるおそれが生じるので、個人情報は、利用目的に応じ正確かつ最新の状態に保たれる必要がある。

① 「個人情報を正確かつ最新の内容に保つ」とは、顧客情報等を管理するデータベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人情報を正確かつ最新の内容に保つよう努めなければならないとの趣旨である。データベースに保存されている個人情報に限らず、他の媒体に保存されている個人情報についても、保存期間の設定をするなど、利用目的の達成に必要な範囲内で正確かつ最新の内容に保つよう努めなければならないものである。
② 「最新の内容に保つよう努める」とは、保有する個人情報を一律に又は常に最新化することを求めるものではなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保することを求める趣旨である。

７．保存期間等（ガイドライン第１０条）

[ガイドライン]
第10条　電気通信事業者は、個人情報を取り扱うに当たっては、原則として利用目的に必要な範囲内で保存期間を定めるものとし、当該保存期間経過後又は当該利用目的を達成した後は、当該個人情報を遅滞なく消去するものとする。

（第10条第1項の解説）
(1) 取得された個人情報については、その目的を達成すれば保存の必要性がなくなることから速やかに消去すべきであるところ、その趣旨を徹底する観点から、利用目的に応じ保存期間を定めることを原則としている。こうすることは、正確性、最新性確保の観点からも望まれるほか、個人が不利益を被る機会を減少させるためにも有用である。ただし、個人情報によっては、一律に保存期間を定めることが難しいものもあり、すべての個人情報について保存期間を定めることまでは要求しないこととする。しかし、この場合でも、利用目的を達成すれば遅滞なく消去すべきものとする。また、保存期間内であっても利用目的を達成した後は消去するものとする。

保存期間については、各事業者が取り扱う個人情報の内容及び業務の実情を踏まえ定めるものであるが、加入者との関係で取り交わす書類等（申込書、利用明細、通信履歴）については洗い出しを行い、特に配慮して適切な保存期間を定める必要がある。

○（好ましい事例）

事例７－１　保存期間の目安の例示として次が考えられる。
・申込情報は、契約解除後の料金精算が終了した後も、クレーム対応に必要とされる場合もあり、契約解除後６ヶ月間保存する。
・利用明細や通信履歴は、料金支払い後もクレーム対応に必要とされる場合もあり、料金支払い後２ヶ月間保存する。
（注）保存期間内であっても利用目的を達成した後は消去しなければならない。また、実際の保存期間は各事業者において具体的に必要性（法令の定め等を含めて考慮する必要がある。）を判断した上で定められるものである。

×（好ましくない事例）

事例７－２　保存期間を定めていない又は利用目的達成後においても正当な理由もなく、長期間個人情報を保存している。

[ガイドライン第10条]
第2項　前項の規定にかかわらず、電気通信事業者は、次の各号に該当すると認めるときは、保存期間経過後又は利用目的達成後においても当該個人情報を消去しないことができる。
一　法令の規定に基づき、保存しなければならないとき。
二　本人の同意があるとき。
三　電気通信事業者が自己の業務の遂行に必要な限度で個人情報を保存する場合であって、当該個人情報を消去しないことについて相当な理由があるとき
四　前3号に掲げる場合のほか、当該個人情報を消去しないことについて特別の理由があるとき。

（第10条第2項の解説）
(2) 保存が求められる「法令の規定」としては、例えば、法人税法（昭和40年法律第34号）第126条、法人税法施行規則（昭和40年大蔵省令第12号）第59条や電話加入権質に関する臨時特例法施行規則（昭和33年郵政省令第18号）第4条等がある。
(3)「本人の同意があるとき」とは、例えば、本人から特に保存しておくよう要請があった場合等が考えられる。なお、「本人の同意」の趣旨については、第15条の解説(2)を参照。
(4)「業務の遂行に必要な限度で個人情報を保存する場合であって、当該個人情報を消去しないことについて相当の理由があるとき」とは、例えば、過去に料金を滞納し利用停止となった者の情報を契約解除後においても保存しておくこと等が考えられる。
(5)「消去しないことについて特別の理由があるとき」とは、例えば、捜査機関から刑事事件の証拠となり得る特定の個人情報（通信の秘密に該当するものを除く。）について保存しておくよう要請があった場合等が考えられる。
(6) なお、通信履歴についての保存期間等に関する取扱いについては、第23条の解説(5)も参照されたい。

≪参考≫
法人税法（昭和40年法律第34号）
第126条
　第121条第1項（青色申告）の承認を受けている内国法人は、財務省令で定めるところにより、帳簿書類を備え付けてこれにその取引を記録し、かつ、当該帳簿書類を保存しなければならない。
2　納税地の所轄税務署長は、必要があると認めるときは、第121条第1項の承認を受けている内国法人に対し、前項に規定する帳簿書類について必要な指示をすることができる。

法人税法施行規則（昭和40年大蔵省令第12号）
第59条
　青色申告法人は、次に掲げる帳簿書類を整理し、7年間、これを納税地（第三号に掲げる書類にあ

っては、当該納税地又は同号の取引に係る法施行地内の事務所、事業所その他これらに準ずるものの所在地）に保存しなければならない。

一　第54条（取引に関する帳簿及び記載事項）に規定する帳簿並びに当該青色申告法人（次項に規定するものを除く。）の資産、負債及び資本に影響を及ぼす一切の取引に関して作成されたその他の帳簿

二　棚卸表、貸借対照表及び損益計算書並びに決算に関して作成されたその他の書類

三　取引に関して、相手方から受け取った注文書、契約書、送り状、領収書、見積書その他これらに準ずる書類及び自己の作成したこれらの書類でその写しのあるものはその写し

2　前項の期間は、帳簿についてはその閉鎖の日の属する事業年度終了の日の翌日から二月（法第75条の2（確定申告書の提出期限の延長の特例）の規定の適用を受けている場合には二月にその延長に係る月数の期間を加えた期間とし、清算中の内国法人について残余財産が確定した場合には一月とする。以下この項において同じ。）を経過した日から、書類についてはその作成又は受領の日の属する事業年度終了の日の翌日から二月を経過した日から、起算する。

3　第1項各号に掲げる帳簿書類のうち次の表の各号の上欄に掲げるものについての当該各号の中欄に掲げる期間における同項の規定による保存については、当該各号の下欄に掲げる方法によることができる。

一　第1項第三号に掲げる書類（帳簿代用書類に該当するものを除く。）のうち国税庁長官が定めるもの	前項に規定する起算の日以後3年を経過した日から当該起算の日以後5年を経過する日までの期間	財務大臣の定める方法
二　第1項各号に掲げる帳簿書類	前項に規定する起算の日から5年を経過した日以後の期間	財務大臣の定める方法

4　前項の表の第一号の上欄に規定する帳簿代用書類とは、第1項第三号に掲げる書類のうち、別表21に定める記載事項の全部又は一部の帳簿への記載に代えて当該記載事項が記載されている書類を整理し、その整理されたものを保存している場合における当該書類をいう。

電話加入権質に関する臨時特例法施行規則（昭和33年郵政省令第18号）

第4条

質原簿は、永久に保存しなければならない。

2 消滅した質権の質原簿につづり込んだ登録用紙は、その登録をまっ消した日から5年間保存しなければならない。

3 附属書類つづり込帳につづり込んだ書類は、これらの書類に係る登録又は届出があった日から5年間保存しなければならない。

○（好ましい事例）

事例７－３　お客様から、身に覚えがない料金請求が来ており、電気通信事業者に対して通信履歴を保存するよう要請があったため、保存期間経過後もそのお客様の通信履歴を保存する。

８．安全管理措置（ガイドライン第１１条）

８－１．技術的保護措置

［ガイドライン］

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。

第2項　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。

（第11条の解説）

(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、それらを処分するために文書裁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。

電気通信事業者は、不特定多数の者が書店で随時に購入可能な電話番号簿で、当該事業者が全く加工していないものを、処分するために溶解や文書裁断機等による処理を行わず破棄し、又は廃品回収に出しても差支えない。

しかし、電話番号簿の発行に関わる電気通信事業者にとって、当該電話番号簿は、自己が保有する個人情報を用いたものであり、その事業者が廃棄処分する場合には、文書裁断や溶解等の処理を行った上で処分すべきである。

電話番号簿自体に個人に関する書き込みをしている場合には、加工したものとみなすべきである。電話をかけた先にチェックを付けたような場合も同様に加工したものとみなすべきである。

８－１－１．アクセスの管理

（第11条の解説）
(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）

個人情報へのアクセスの管理として、具体的には次のような措置をとることとする。

ア．アクセス権限者の限定

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報へのアクセス権限を必要最小限とすることとする。

また、従業者(注)が異動・退職等によりアクセス権限が失われたときは、直ちにアカウントを無効にするとともに、長期にアクセス権限が放置されることを防止するために有効期間を設定する等定期的に有効確認を行うこととする。

さらに、委託先の従業者や再委託先等の従業者に対し、アクセスを認める場合にも、従業者と同様に、アクセス権限の限定や有効確認等を行う必要がある。

（注）「従業者」とは、電気通信事業者の組織内にあって直接間接に事業者の業務に従事している者をいい、電気通信事業者との間の雇用関係の有無は問わないので、雇用関係にある従業員（正社員、契約社員、嘱託社員、パートタイマー、アルバイト等）及び役員（取締役、執行役、監査役、理事、監事等）のほか派遣労働者も含まれる。

＜措置の例＞

- 従業者の情報とアカウントを一元的に管理し、人事異動や組織変更等がタイムリーに反映されるシステムの導入（アカウントの重複や削除漏れを防止）
- アクセスのためのＩＣカード等の認証デバイスシステムの導入

イ．アクセス状況の監視体制

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報へのアクセス者が特定できるアクセス履歴（使用者、使用・エラー履歴、不規則利用等）を残し、これを監視するとともに、必要な範囲内でアクセスログの保存期間を定めて、保存することとする。

＜措置の例＞

- アクセス時ステータスが確認可能なＩＣカード等の認証システムの導入
- アクセス記録の長期（又は無期限）保存
- 不正アクセスを遮断可能な監視ツール等の導入

- 不正アクセスへの防御性を高めるためのネットワークのシステムの脆弱性の定期的な調査の実施
- 不正侵入検知装置（ＩＤＳ）等の導入
- 個人情報を取り扱うシステムへのインターネット経由のアクセスの制限（セキュリティーを確保のためのシステムの導入やアクセスの規制等）

ウ. パスワードの定期的変更

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報へのアクセスが可能なシステム又は端末に対するパスワードについて有効期間を設定する等により定期的に有効確認を行うこととする。

＜措置の例＞

- パスワードの有効期間（１～３ヶ月）を定め、期限までに変更を促し、必ず変更させるようなシステムの導入

エ. 入退室管理

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報を取り扱う敷地、ビル、事務室、設備等の設置環境に関して、その取り扱う個人情報の内容、形態、規模に応じて区分毎の入退室権限を設定するとともに各種管理システム等を通じて入退室管理を行うこととする。

＜措置の例＞

- ビルや部屋、端末、ネットワーク、ファイル等、個人情報に対するあらゆるレベルのアクセスについて、ＩＣカード等の認証デバイスを用いて管理し、すべての証跡が個人を特定できる形式で必要な期間保存されるシステムの導入

○（好ましい事例）

事例８－１　社員の情報とアカウントを一元的に管理し、人事異動や組織変更等がタイムリーに反映される仕組みを導入する等して、アカウントの重複や削除漏れを防止するよう対処している。

事例８－２　パスワードの有効期間（１～３ヶ月）を定め、システム上期限までに変更を促して必ず変更させるような仕組みを導入している。

事例８－３　ビルや部屋、端末、ネットワーク、ファイル等、個人情報に対するあらゆるレベルのアクセスについて、ＩＣカード等の認証デバイスを用いて管理し、すべての証

跡が個人を特定できる形式で必要な期間保存される仕組みを導入している。

事例８－４　不正なアクセスに対し、監視ツール等を利用して監視するとともにそうした疑いのある不正なアクセスを遮断している。

事例８－５　不正なアクセスを防ぐため、ネットワークやシステムの脆弱性を定期的に調査して、防御性を高めるように対処している。

事例８－６　不正侵入検知装置（ＩＤＳ）等を活用することにより、不正パケットを常時監視し、内部からの情報漏えいを防止している。

事例８－７　コンピューターウィルス・ワームのチェックツール及びそのパターンファイルを常に最新に保ち、感染状況等を常時監視して迅速に対策を講じることができる体制を構築する等して、個人情報が漏えいしないよう対処している。

事例８－８　インターネット経由で個人情報を取り扱うシステムにアクセスすることについて、セキュリティーを確保するとともにそのアクセスを適切に管理している。

×（好ましくない事例）

事例８－９　個人情報へのアクセスログを保存しない、又は、保存したとしても数日で削除されてしまう。

８－１－２．持出し手段の制限

（第11条の解説）
⑵ 技術的保護措置とは、・・・
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）

個人情報の持出し手段の制限として、具体的には次のような措置をとることとする。

ア．みだりに外部記録媒体へ記録することの禁止

電気通信事業者は、従業者が業務に必要な範囲を超えて個人情報をパソコンや外部記録媒体（従業者が持ち込んだ媒体を含む。）に記録することを禁止することとする。

＜措置の例＞

- 個人情報を外部記録媒体へ記録するパソコン上の操作（個人情報データベースからのダウンロードやファイルサーバ等からのコピー及び印刷等。）について常時監視システムを導入する。
- 個人情報へのアクセスが可能なシステム又はパソコンに、ＵＳＢメモリ、ＦＤドライブ等の外部記録媒体の使用を限定するソフトウェアを導入する。
- 個人情報へのアクセスが可能なシステム又はパソコンに、ＵＳＢメモリ、ＦＤドライブ等の外部記録媒体の接続装置を装着しない。
- 業務上の必要性からやむをえず個人情報を外部記録媒体に記録する場合は、個人情報を分割し組み合わせないと復元できず、かつ、その分割したそれぞれのデータ単独では元の情報を全く復元できない仕組み等外部記録媒体の紛失等に対して適切な対処を施す。
- サーバに格納した個人情報に、パソコンや携帯電話等の端末からアクセスしても、それらの端末には個人情報が残らないシステムを導入する。

イ．パソコンの持出し制限

電気通信事業者は、個人情報を記録したパソコンの持出しに関する社内規則（持出しの許されるパソコンの特定、起動時のパスワード設定等）を定め、適正に管理することとする。

ウ．私物パソコン等の使用の制限

従業者の私物のパソコンや外部記録を業務に使用することを原則として禁止することとし、やむを得ず私物パソコン等の使用を認める場合には、会社の業

務用のパソコン等と同様の安全管理措置が講じられていることを厳重に確認することとする。

エ．電子メール使用ルール

個人情報を外部に漏えい等する危険を避けるための電子メールの使用ルールを定めるとともに、メールフィルタリングや送信メールのログの記録化等、これを担保するシステムを導入するなどの対策を講じることとする。

＜電子メールの使用ルールの例＞

- 私用メールは一切禁止する。
- 社外への複数配信の禁止（複数配信する必要がある場合には、適切な取扱いを図るよう十分注意しつつＢＣＣやメール配信システムを使用）
- 携帯電話や他のパソコンへの自動転送禁止
- 個人アドレスへの業務メールの転送禁止
- 個人情報を含む電子メールの送信時の、暗号化やパスワードの設定の必須化
- 社外メール配信時の複数従業者によるチェック

オ．社内と社外の間の電子メール監視

電気通信事業者は、必要に応じ、あらかじめ社内規則等に規定した上で、従業者の社内と社外との間の電子メールを監視するなどの措置を講じることとする。

ただし、その場合は従業者のプライバシー保護に十分留意するものとする。また、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また、その規定を定めたときは、従業者に周知することが望ましい。

カ．消去の徹底

電気通信事業者は、個人情報を記録した媒体（パソコン、外部記録媒体、紙等）を廃棄する場合は、個人情報の消去を徹底することとする。

○（好ましい事例）

事例８－１０　個人情報を外部記録媒体へ記録するパソコン上の操作（個人情報データベースからのダウンロードやファイルサーバ等からのコピー及び印刷等。）について常時監視することで、個人情報が漏えいすることを防止している。

事例８－１１　業務上の必要性からやむをえず個人情報を外部記録媒体に記録する場合は、個人情報を分割し組み合わせないと復元できず、かつ、その分割したそれぞれのデ

ータ単独では元の情報を全く復元できない仕組みを採用するなど外部記録媒体の紛失等に対して適切な対処を施している。

事例８－１２　サーバに格納した個人情報に、パソコンや携帯電話等の端末からアクセスしても、それらの端末には個人情報が残らない仕組みを導入することで、故意の場合のみならず、本人が意図しないにもかかわらず自己の端末に情報が蓄積される形態も含め、個人情報の外部持出しを防止している。

事例８－１３　不正侵入検知装置（ＩＤＳ）等を設置することにより、情報漏えいに繋がる通信（社内で監視しているメールサーバを経由しない通信等(注)）を適切に検知し、対処を行える仕組みを設けている。

(注)社内で監視しているメールサーバを経由しない通信等

インターネット上のWebメールを利用したメール通信、外部とのチャットやメッセンジャ通信、ウイルスやスパイウェアの通信等をいう。

事例８－１４　個人情報へのアクセスが可能なシステム又はパソコンに、ＵＳＢメモリ、ＦＤドライブ等の外部記録媒体の使用を限定するソフトウェアを導入している。

×（好ましくない事例）

事例８－１５　個人情報が含まれたデータベースについて、外部記憶装置(端末も含む)にダウンロードすることなく参照できるにもかかわらず、データを外部記録装置に記録する。

事例８－１６　個人情報が含まれたデータベースから必要な情報のみを抽出する機能があるにもかかわらず、すべてのデータを外部記憶装置に記録する。

事例８－１７　個人情報が含まれたデータについて、必要以上の部数をプリントアウトする。

８－１－３．外部からの不正アクセスの防止

（第11条の解説）
⑵ 技術的保護措置とは、･･･
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）

外部からの不正アクセスの防止のための措置として、具体的には次のような措置をとることとする。

ア．ファイアウォールの設置

電気通信事業者は、不正アクセスを防止するために、ネットワークに接続する情報システムには、ファイアウォール、不正侵入検知装置（ＩＤＳ）等の不正アクセス防止機器を設置するなどの対策を講じることとする。

イ．Ｗｉｎｎｙ等ファイル交換ソフト等の使用制限

Ｗｉｎｎｙ等ファイル交換ソフトや、会社が安全性を確認したソフトウェア以外のソフトを、業務用パソコンにインストールすることや使用することを禁止することとし、定期的又は恒常的に監視を行うこととする。

○（好ましい事例）

事例８－１８　インターネットに接続する情報システムに対し、最新のセキュリティー情報に基づいてファイアウォール、不正侵入検知装置（ＩＤＳ）等の設定を常に適正に保ち、常時監視できるような仕組みを導入することにより個人情報の漏えい等を防止している。

８－１－４．情報セキュリティーに関する基準の活用

（第11条の解説）
⑵ 技術的保護措置とは、・・・
（①～③）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。

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、実施することとは、具体的には、電気通信事業者は、必要に応じ、国内外の工業標準化の促進を活動目的とした団体等から発行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、適切な内部規程・マニュアルを策定し、実施することとする。

８－１－５．技術基準の適合維持義務

（第11条の解説）
⑵ 技術的保護措置とは、・・・
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。

電気通信事業者の保有する個人情報を格納する装置が、電気通信事業法第４１条に定める事業用電気通信設備に該当する場合は、当該装置が事業用電気通信設備規則（昭和６０年郵政省令第３０号）の定める技術基準を満たさないことによって損傷又は破壊されることのないようにすることとする。

８－２．組織的保護措置

８－２－１．従業者・委託先の責任と権限の明確化

（第11条の解説）
⑶ 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
（･･･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、それらの規定を参照されたい。）

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とは、具体的には、次のような措置をとることとする。

ア．従業者の責任と権限の明確化

電気通信事業者は、その雇用する従業者に対しては就業規則において、雇用関係にない従業者に対してはその雇用者との契約において、従業者の責任を明確にすることとする。また、内部規程中に個人情報を取り扱うことができる従業者を決める権限者を明らかにすることとする。

イ．委託先の責任と権限の明確化

電気通信事業者は、委託先に業務を委託する契約中に、個人情報の保護・秘密保持に関する規定を置くこととする。

８－２－２．内部規程・マニュアルの策定と監査

（第11条の解説）
(3) 組織的保護措置とは、･･･
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
（･･･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、それらの規定を参照されたい。）

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ともに、その遵守の状況について適切な監査を行うこととは、具体的には、次のような措置をとることとする。

ア．安全管理に関する内部規程・マニュアルの策定

電気通信事業者は、事業内容、その取り扱う個人情報の内容、形態、規模に応じて安全管理に関する内部規程・マニュアルを策定することとする。

なお内部規程・マニュアルには、個人情報の適正な取扱いの確保に必要な体制に関する規定、物理環境に関する規定、情報システムに関する規定、インシデントに関する規定、監査に関する規定等を置くこととする。

イ．安全管理に関する適切な監査

電気通信事業者は、安全管理に関して定めた内部規程・マニュアルの遵守状況を、自己診断、内部監査、外部監査等のいずれか又は各種監査方法を組み合わせ、定期的かつ効率的に監査することとする。

８－２－３．従業者・委託先との秘密保持契約締結

（第11条の解説）
⑶ 組織的保護措置とは、･･･
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
（･･･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、それらの規定を参照されたい。）

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とは、具体的には、次のような措置をとることとする。

ア．従業者との内部規程・マニュアル遵守の誓約

電気通信事業者は、従業者に対し、その就労の開始時において、安全管理に関する従業者の責任と権限を明確にした内部規程・マニュアルについて十分な説明又は教育・訓練を施したうえで、その遵守を誓約させることとする。

イ．委託先との秘密保持契約の締結

電気通信事業者は、委託先に業務を委託する契約中に、委託先に委ねる個人情報の内容、形態、規模に応じて、個人情報の保護・秘密保持に関する規定を置くこととする。

８－２－４．教育研修

（第11条の解説）
(3) 組織的安全管理措置とは、･･･
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、それらの規定を参照されたい。

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とは、具体的には、次のような措置をとることとする。

ア．就労の開始時における個人情報保護に関する教育研修

電気通信事業者は、従業者に対し、就労の開始時に個人情報保護に関する教育研修を実施するものとし、当該教育研修の実施にあたっては、教育研修の実施効果及び監査等の目的を考慮して、教育研修の体系、実施計画を立案するものとする。

イ．年１回程度の教育研修

電気通信事業者は、すべての従業者に対し、少なくとも年１回程度の個人情報の保護に関する教育研修を実施するものとする。（９－１－２．従業者への教育研修参照のこと）

８－３．持出時の安全管理措置を講じる際の考え方等

（第11条の解説）

(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一水準維持、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。

個人情報の入ったパーソナルコンピュータや外部記録媒体等を社外へ持ち出す場合には、パーソナルコンピュータ等が紛失、盗難することにより個人情報が漏えいするリスクがあることから、次のような点に留意して、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。

① リスクの評価では、持ち出す個人情報の種類、内容やその分量、持ち出す従業者の範囲や持ち出す方法、社内での管理状況等の関連する状況を踏まえ、ど

のようなリスクがどこで生じるのか等、個人情報を社外へ持ち出した場合に想定される具体的なリスクを網羅的に整理し評価することが必要である。

② 「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」とは、導入コストをかけて部分的にセキュリティー強度を強固にしても、相対的にセキュリティー強度の弱い部分があれば、その部分から問題が生ずるおそれがあるため、技術的にセキュリティー強度の最も弱い部分を把握し、その部分に対応する措置が十分なものなのかを検討することが必要であるとの趣旨である。

③ 「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」とは、措置を講ずることによる利便性への影響及び導入コストと、持ち出された個人情報の安全性の双方を勘案することが重要であり、一般に、利便性や導入コストと安全性とはトレードオフの関係にあるため、評価したリスクについて、利便性や導入コストと安全性の双方のバランスを判断して適切な措置を決定することが必要であるとの趣旨である。

④ 決定した措置が適切に運用されることを確実にするために、内部規程等が遵守されているかどうかの定期的な監査や、従業員に対する定期的な研修の実施等に努めることが必要である。また、リスク評価や必要とされる措置について適宜に見直しを行うことが必要である。

⑤ 個人情報を持ち出す場合には、適切な技術的保護措置を講じているかどうかには拘らず、紛失や盗難に遭わないように、パーソナルコンピュータ等が適切に管理されるようにすることや、持ち出す個人情報は、業務上必要最低限の範囲にすることが必要である。

⑥ 「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が必要であるが、これらの個人情報の例には、通信の秘密に該当する情報や銀行口座番号、クレジットカード情報等のほか、ガイドライン第４条第２項で取得を制限しているいわゆるセンシティブ情報が含まれる。

ワイヤレスブロードバンド環境の進展や持ち出した情報資産の安全性を確保可能とするサービスの登場により、個人情報をパーソナルコンピュータや外部記憶媒体等で社外に持ち出す場合に、漏えいが発生した場合でも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を講じることも可能になってきている。

なお、パーソナルコンピュータや外部記憶媒体等の紛失等に際し、漏えい等の発生した個人情報に対して適切な技術的保護措置が講じられていた場合には、本人への通知、公表、総務省への報告に関する手続を簡略化することが可能と

されている。（ガイドライン２２条参照）

個人情報をパーソナルコンピュータや外部記録媒体等で社外に持ち出す場合に想定されるリスクと技術的対応策、求められる安全管理措置については、総務省「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」で検討され第二次提言として公表されている。（平成２２年５月）

具体的な安全管理措置の取組については、参考資料３－２総務省「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」第二次提言の抜粋(注)を参照されたい。

（注）参考資料３－２は総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言から次の部分を抜粋している。

Ⅲ　安全管理措置に関する検討について

2. 想定されるリスクと技術的対応策

3. 求められる安全管理措置

９．従業者及び委託先の監督（ガイドライン第１２条）

９－１．従業者の監督

９－１－１．従業者に対する監督責任

[ガイドライン]
第12条　電気通信事業者は、その従業者（派遣労働者を含む。以下同じ。）に個人情報を取り扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行うものとする。

（第12条第1項の解説）
(1) 第1項は、電気通信事業者が、個人情報を取り扱うに当たり、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従業者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。
「従業者」とは、電気通信事業者の組織内にあって直接間接に事業者の業務に従事している者をいい、電気通信事業者との間の雇用関係の有無は問わないので、雇用関係にある従業員（正社員、契約社員、嘱託社員、パートタイマー、アルバイト等）及び役員（取締役、執行役、監査役、理事、監事等）のほか派遣労働者も含まれる。
従業者に対する必要かつ適切な監督には、従業者との秘密保持契約の締結（派遣労働者については、派遣元との秘密保持契約の締結及び派遣元と派遣労働者の間の適切な秘密保持契約の締結の確保等の措置）等が含まれる。

従業者との秘密保持契約の締結にあたっては、次の点に注意すべきである。

＜直接雇用社員の場合＞
誓約書・念書の提出を求める。

＜派遣社員の場合＞
派遣元への誓約書等の提出を派遣契約条件に含める。直接派遣社員に誓約書等の提出を求める場合には、罰則の規程がない誓約書等とする。

＜委託先従業者＞
委託先への誓約書等の提出を委託契約に記載する。

電気通信事業者が、その従業員に提出を求める秘密保持誓約書の就業時と退職時それぞれの記載例を参考資料１の例２及び例３に示す。これらは、電気通信事業者が誓約書の書式を作成するにあたっての参考として示すものである。

電気通信事業者は、その従業者に個人情報を取り扱わせるにあたっては、当該個人情報の安全管理が図られるよう、当該従業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。

したがって、電気通信事業者は内部に監督部署を設けるとともに、常に個人情報の取扱いに対して細心の注意を払い、万が一個人情報の漏えいが発生した場合の対応や個人情報の漏えいを防止するための安全管理措置を定めた規程を作成し、それにのっとった運営を行うことが必要である。規程には従業者の秘密保持に係る条項の記載をすべきである。また、定期的な監査を実施し、監督部署が監査に係る記録を作成、保存することが重要である。（規程の作成にあたっては「８．安全管理措置関連」を参考にすると良い。）

なお、当該規程は必要に応じて見直しをするべきである。

○（好ましい事例）

事例９－１　電気通信事業者は、従業者に対する必要かつ適切な監督を行うために、監督部署を設置するとともに、個人情報保護に係る規程を作成し、それにのっとった運営を行うこと。

×（好ましくない事例）

事例９－２　事業者が、従業者を監督する部署を設置していない上、個人情報保護に係る規程にのっとった運営を行えていない場合。

９－１－２．従業者への教育研修

[ガイドライン第12条]
第2項　電気通信事業者は、安全管理措置の実施その他の個人情報の適正な取扱いの確保のため、その従業者に対し、必要な教育研修を実施するものとする。

（第12条第2項の解説）
(2) 第2項は、安全管理措置の実施その他の個人情報の適正な取扱いの確保のため、電気通信事業者は、従業者に対し、必要な教育研修を実施することを規定している。教育研修の内容としては、安全管理に関する内部規程・マニュアルの周知等が考えられる。

電気通信事業者は安全管理措置の実施その他の個人情報の適切な取扱いの確保のため、すべての従業者に対し、少なくとも年１回程度の個人情報の保護に関する教育研修を実施しなければならない。教育研修の内容としては法やガイドラインの説明、通信の秘密に係る電気通信事業法の規定の説明、各電気通信事業者において講じている安全管理措置の具体的な内容（パスワードの変更に関する事項や個人情報の取扱いのマニュアルなど）、安全管理措置に違反した場合に科される処分などの項目を含めるべきである。

また、教育研修の受講状況を把握し、確認テスト等により、研修の成果を確認することも重要である。

従業者を監督する部署の担当者及び監督する立場の者は、最新動向を把握する上で年間 1 回以上社外講師等の教育研修を受講する必要がある。教育研修内容は最新の技術的安全管理措置、組織的安全管理措置を修得することが前提となり次の機関等が実施する教育研修を受講することが望ましい。

- 官公庁が主催又は推奨する個人情報保護の教育研修
- 認定個人情報保護団体が主催又は推奨する個人情報保護の教育研修等

○（好ましい事例）

事例９－３　電気通信事業者は、安全管理措置の実施その他の個人情報の適切な取扱いの確保のため、教育研修の実施に関する事項を個人情報保護に係る規程などに定め、これを実施する（例えば、従業者を監督する部署が実施する教育研修を従業者に受講させる等）。

×（好ましくない事例）

事例９－４　会社として、教育研修について何も定めていない。また、教育研修の実施に関する事項を定め研修を実施しているが、従業者の受講状況を把握していない。

９－２．委託先の監督

９－２－１．必要かつ適切な監督

[ガイドライン第12条]
第3項　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。

（第12条第3項の解説）
（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。

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、委託先に対する必要かつ適切な監督を行わなければならない。

「必要かつ適切な監督」には、委託契約において委託元である電気通信事業者が定める安全管理措置の内容を契約に盛り込むとともに、当該契約の内容が遵守されていることを、あらかじめ定めた間隔で定期的に確認することも含まれる。

電気通信事業分野における具体的な委託先の例としては、次のような者があるが、これに限定されるものではない。

- 契約代理業者（電気通信サービス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）
- ダイレクト・メール等の宛名等の印刷・発送代行業者
- 個人情報のデータ入力、編集、出力等の処理を行う者
- 料金の回収や決済を代行する者
- 請求書など個人情報を含む文書等の送達を行う者(注)
- コールセンター等で苦情・相談の受付を代行する者
- 回線設置工事等を行う者

（注）個人情報を含む文書等を郵便や宅配便等で送付する場合、電気通信事業者は郵便局や宅

配業者等に個人情報の取扱いを委託していると解されている。
　しかし、郵便局や宅配業者等は、通常は送付物の中に個人情報が含まれているかどうかを認識することなく個人情報を取り扱っているので、個人情報保護法の義務規定が適用されないものと解されている。

×（好ましくない事例）

事例９－５　個人情報の安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託している。

９－２－２．委託契約等

[ガイドライン第12条]
第4項　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。

（第12条第4項の解説）
(4) 第4項は、第3項の委託にあたって、個人情報を適正に取り扱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。

個人情報の取扱いを委託する場合に契約書への記載が望まれる事項として、次の項目があげられる。また、委託先が再委託をした場合であって、再委託先において当該委託に係る個人情報の漏えいが発生したときは、委託元が責任を負うこともあり得るので、再委託を許す場合は注意を要する。

- 個人情報の目的外利用の禁止
- 個人情報の第三者提供の禁止
- 委託元及び委託先の責任に関する事項
- 個人情報の安全管理に関する事項
- 再委託に関する事項
- 秘密保持に関する事項
- 従業者の教育に関する事項
- 個人情報の取扱状況に関する委託元への報告内容及び頻度に関する事項
- 契約内容が遵守されていることの確認方法
- 契約内容が遵守されていなかった場合の措置
- 委託業務終了後の個人情報の取扱い（返却、消去等）に関する事項
- 個人情報の漏えい等が発生した場合の報告及び連絡に関する事項

契約書の記載方法としては、委託契約そのものに個人情報保護に関する事項を記載する方法と委託契約には個人情報保護に関する取り決めは別の覚書等によることを明記の上、個人情報の取扱いに関する別の覚書等を締結する方法など

がある。

電気通信事業者が、業務委託先と結ぶ個人情報保護に関する覚書の記載例を参考資料１の例４に示す。これは、個人情報保護に関する覚書が委託先との自由な合意に基づき締結されるにあたっての参考として示すものである。

×（好ましくない事例）

事例９－６　個人情報の取扱いに関して定めた安全管理措置の内容を委託先に指示せず、結果、委託先が個人情報を漏えいした場合。

事例９－７　再委託の条件に関する指示を委託先に行わず、かつ委託先の個人情報の取扱状況の確認を怠り、委託先が個人情報の処理を再委託し、結果、再委託先が個人情報を漏えいした場合。

９－３．従事者の責務

[ガイドライン第12条]
第5項　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。

（第12条第5項の解説）
(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。

電気通信事業者及びその従業者には個人情報を適正に取り扱うべき責務がある。電気通信事業者はその従業者がよくその意味を理解できるよう教育・研修等を実施するとともに守秘義務に係る誓約書・念書等の提出や個人情報保護を明示している就業規則の遵守を求めることが望ましい。また、従業者が退職する場合には、退職後も機密を保持することについての誓約書・念書等の提出を求めることが望ましい。

また、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（委託先及びその従業者）も、電気通信事業者及びその従業者と同じく個人情報を適正に取り扱うべき責務がある。電気通信事業者は委託先と個人情報の取扱いに関する秘密保持の契約等を結ぶとともに委託先に委託先従業者からの守秘義務に係る誓約書・念書等の取得を求めることが望ましい。

○（好ましい事例）

事例９－８　退職者による個人情報漏えい防止のため、退職時に機密保持の誓約をさせるとともに、従業者を監督する部署等の立会いのもと、退職者が在職中取り扱っていた個人情報の消去や個人情報に関する資料の引継ぎを実施する。

×（好ましくない事例）

事例９－９　退職者が在職中に取り扱っていた個人情報を消去したことの確認や、個人情

報に関する資料等（外部に持ち出していたデータ等を含む。）の所在確認や引継ぎを行わない。

事例９－１０　従業者が業務上取り扱っている個人情報の中に、たまたま昔の知り合いの氏名・電話番号が含まれているのを知り、当該情報を利用して連絡をとる。

１０．個人情報保護管理者（ガイドライン第１３条）

[ガイドライン]
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。

（第13条の解説）
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。

（注）
電気通信個人情報保護推進センターでは、対象事業者の次の申込項目の内容に変更があった場合、その変更の届を行うことを対象事業者に求めている。
これら項目は、電気通信個人情報保護推進センターと対象事業者が協力して個人情報保護の推進にあたるための基本的な情報共有であり、対象事業者は、変更の届を遅滞なく電気通信個人情報保護推進センターに行う必要がある。

・会社名
・代表者氏名
・本社住所
・所属事業団体
・事業内容
・サービス名称
・公表窓口
・保護管理者
・連絡窓口

１１．プライバシーポリシー（ガイドライン第１４条）

[ガイドライン]
第14条　電気通信事業者は、プライバシーポリシー（当該電気通信事業者が個人情報保護を推進する上での考え方や方針をいう。）を公表し、これを遵守するものとする。

（第14条の解説）
(1) 本条は、電気通信事業者の個人情報保護についての社会の信頼を確保するため、電気通信事業者は自らの個人情報保護を推進する上での考え方や方針をプライバシーポリシーとして公表し、これを遵守するものとすることを規定したものである。
(2) プライバシーポリシーは、それぞれの電気通信事業者が、分かりやすい表現で記載すべきものであるが、プライバシーポリシーに記載すべき事項としては、次のようなものが考えられる。
① 個人情報保護法及び通信の秘密に係る電気通信事業法の規定その他の関係法令の遵守
② 本ガイドラインの遵守
③ 第16条第1項各号に定める公表すべき事項
(i) 電気通信事業者の名称
(ii) 個人情報の利用目的
(iii) 利用目的の通知又は開示若しくは訂正等の本人からの求めに応じる手続
(iv) 苦情の申出先
(v) 認定個人情報保護団体の名称及び苦情の解決の申出先
④ 第11条の安全管理措置に関する方針
⑤ 利用者の権利利益の保護に関する事項
(i) 保有個人情報について本人から求めがあった場合には、ダイレクト・メールの発送停止など、自主的に利用停止等に応じること。
(ii) 委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めること
(iii) 電気通信事業者がその事業内容を勘案して利用者の種類ごとに利用目的を限定して示したり、電気通信事業者が本人の選択による利用目的の限定に自主的に取り組むなど、本人にとって利用目的がより明確になるようにすること
(iv) 個人情報の取得元又はその取得方法（取得源の種類等）を、可能な限り具体的に明記すること

プライバシーポリシーは、電気通信事業者が個人情報保護を推進する上での考え方や方針をいう。実際にプライバシーポリシーをどういう位置づけにするかにより、具体的な形式や表現については様々なバリエーションがあると考えられるが、いずれにしても利用者にとって分かりやすいものであることが望まれる。この点、ガイドライン第１６条第１項各号に定める公表すべき事項を、プライバシーポリシーにすべて網羅的に記述すると、かえって分かりにくいもの

となることも考えられる。

プライバシーポリシーを作成する際の留意点は、次のとおりである。

① 個人情報に関連する法令などの遵守

個人情報保護法及び通信の秘密に係る電気通信事業法の規定その他の関連法令並びにガイドラインを遵守する考え方や方針を公表することが必要である。

② 個人情報の適正な取扱いに関する方針

利用目的の特定、利用目的による制限、適正な取得、保存期間、安全管理措置、従業者及び委託先の監督、第三者提供の制限、開示等の手続、苦情の処理、漏えい等が発生した場合の対応など個人情報の適正な取扱いに関する考え方や方針を公表することが必要である。

③ 利用者の権利利益の保護に関する取組

電気通信事業者は、利用者の権利利益保護に取り組むことが求められる。次のようにプライバシーポリシーに具体的な取組を記載するか、又は、保護のための取組を促進する考え方や方針を公表することが望ましい。

（ｉ） ダイレクト・メールの発送停止や電話勧奨の停止等に応じる場合には、その旨ホームページやパンフレットで公表するとともに、停止の申出の受付先を整備することが望ましい。

○（好ましい事例）

事例１１－１　電気通信サービスの契約者には、契約時に当該サービスにかかる情報のほか、自社が提供する他のサービスについての営業情報をダイレクト・メールや電話でお伝えすることの同意を得ていたが、ホームページで次の周知を行い、停止の申し出を受け付けることにした。

「お客様がダイレクト・メールによる宣伝物の送付や電話による新規サービスのご案内等を希望されない場合、当社に対しその中止及び再開を申し出ることができます。

中止のお申出は、次の連絡先又は当社窓口にお申出下さいますようお願い致します。

連絡先：××××」

（ii） 委託処理の透明化の取組

電気通信事業者は、委託の有無や委託する事務の内容等を明らかにするように努め、次のような委託処理の透明化の取組をホームページ等で公表し、これを実施することが求められる。

≪公表の場合の例≫

- 当社は、各種商品・サービスの販売・受付業務・故障修理業務・料金関連業務・マーケティング業務その他の業務において、個人情報の取扱いの全部又は一部を委託する場合があります。この場合、当社は、個人情報を適正に取り扱うと認められるものを選定し、委託契約において、安全管理、秘密保持、再委託の条件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、必要かつ適切な監督を実施します。
- 当社が、業務の一部を委託する場合において、当該業務委託先から受領することとなる個人情報は、その業務に必要となる範囲内で利用します。
- 当社は、他の事業者から他の事業者の商品・サービスの販売・取次等の委託を受けることがあります。その委託の実施に当たって取り扱うこととなる個人情報は、当該委託された業務の実施に必要となる範囲内で利用します。

（ⅲ）利用目的の限定の取組

「２－１．利用目的の特定」の措置を確実に行うことが重要である。

また、ダイレクト・メールの発送停止や電話勧奨の停止等に応じることは、本人の選択による利用目的の限定のひとつと考えられる。

（ⅳ）個人情報の取得元等の明記

契約者やアンケート応募者等本人からその個人情報を取得する場合以外に、次のような個人情報の取得を行っている場合には、その旨を通知・公表するか、又は、問合わせに即答できるようにしておくことが望ましい。

- 他の事業者から個人情報の第三者提供を受ける場合
- 市販の電話番号簿等から個人情報を取得する場合
- 個人情報の委託を受けて委託元から個人情報の提供を受ける場合

④ 継続的改善の実施

個人情報保護に必要な管理体制を継続的に改善する考え方や方針を公表することが望ましい。

⑤ 関連情報の参照

ホームページ上で公表する場合は、プライバシーポリシーと利用目的等をリンクさせるなどの工夫をし、利用者により分かりやすいものとなるよう工夫すべきである。

⑥ プライバシーポリシーに関する問合わせ窓口

プライバシーポリシーの下に、プライバシーポリシーに関する問い合わせ窓口の連絡先を表示することが望ましい。なお、個人情報取扱窓口や苦情窓口を含め、問い合わせ窓口が多岐にわたり読み手に混乱を招く恐れがある場合は、適宜、窓口表示を統一する等の方法をとることも考えられる。

プライバシーポリシーの記載例を、参考資料１の例５に示す。これは、電気通信事業者が個人情報保護を推進する上での考え方や方針を公表するにあたっての参考として示すものである。

１２．第三者提供の制限（ガイドライン第１５条）

１２－１．第三者提供の制限と例外

[ガイドライン]

第15条　電気通信事業者は、次の各号のいずれかに該当する場合を除くほか、あらかじめ本人の同意を得ないで、個人情報を第三者に提供しないものとする。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

１２－１－１．原則と例外

（第15条第1項の解説）

(1) 第1項は、個人情報は、原則として本人の同意なく、第三者に提供できないことを規定したものである。ただし、自己又は他人の権利利益や社会公共の利益のために第三者提供が要請される場合もあるので、そうした場合を第1項各号に例外として定めている。

１２－１－２．本人の同意（契約約款による同意）

（第15条第1項の解説）

(2)「本人の同意」については、個別の同意がある場合だけでなく、電気通信サービスの提供に関する契約約款において、個人情報の第三者提供に関する規定が定められており、当該契約約款に基づき電気通信サービス提供契約を締結している場合、当該規定が私法上有効であるときも、「本人の同意」がある場合と解される。

この理は、契約約款が変更される場合も変わりはないので、契約約款の変更により個人情報の第三者提供に関する規定が設けられた場合であっても、当該変更が私法上有効であり変更前に契約締結を行った当事者にも変更後の規定が効力を有すると判断される場合には、「本人の同意」がある場合と解される。

なお、同意は有効なものでなければならないので、民法（明治29年法律第89号）第90条の公序良俗に反する場合や同法第95条の要素の錯誤がある場合、消費者契約法（平成12年法律第61号）第10条の消費者の利益を一方的に害するものとされる場合など同意が私法上無効とされる場合は、有効な同意があるとは言えないので、同意がある場合とは言えないことは当然である。

また、無制限に第三者提供を認める規定等契約約款の規定が、利用者の利益を阻害していると認められるときは、電気通信事業法上の業務改善命令の対象となりうる。

≪参考≫

民法（明治29年法律第89号）

第90条

公の秩序又は善良の風俗に反する事項を目的とする法律行為は、無効とする。

第95条

意思表示は、法律行為の要素に錯誤があったときは、無効とする。ただし、表意者に重大な過失があったときは、表意者は、自らその無効を主張することができない。

消費者契約法（平成12年法律第61号）

第10条

民法、商法その他の法律の公の秩序に関しない規定の適用による場合に比し、消費者の権利を制限し、又は消費者の義務を加重する消費者契約の条項であって、民法第一条第二項に規定する基本原則に反して消費者の利益を一方的に害するものは、無効とする。

１２－１－３．法令に基づく場合

（第15条第1項の解説）

⑶「法令に基づく場合」とは、例えば、裁判官の発付する令状により強制処分として捜索・押収等がなされる場合や法律上の照会権限を有する者からの照会（刑事訴訟法（昭和23年法律第131号）第197条第2項、少年法（昭和23年法律第168号）第6条の4、弁護士法（昭和24年法律第205号）第23条の2、特定電子メールの送信の適正化等に関する法律（平成14年法律第26号、以下「特定電子メール法」という。）第29条等）がなされた場合である。前者の場合には、令状で特定された範囲内の情報を提供するものである限り、提供を拒むことはできない。これに対し、後者の場合には、原則として照会に応じるべきであるが、電気通信事業者には通信の秘密を保護すべき義務もあることから、通信の秘密に属する事項（通信内容にとどまらず、通信当事者の住所・氏名、発受信場所及び通信年月日等通信の構成要素並びに通信回数等通信の存在の事実の有無を含む。）について提供することは原則として適当ではない。他方、個々の通信とは無関係の加入者の住所・氏名等は、通信の秘密の保護の対象外であるから、基本的に法律上の照会権限を有する者からの照会に応じることは可能である。もっとも、個々の通信と無関係かどうかは、照会の仕方によって変わってくる面があり、照会の過程でその対象が個々の通信に密接に関係することがうかがわれる場合には、通信の秘密として扱うのが適当である。いずれの場合においても、本人等の権利利益を不当に侵害することのないよう提供等に応じるのは、令状や照会書等で特定された部分に限定する等提供の趣旨に即して必要最小限の範囲とすべきであり、一般的網羅的な提供は適当ではない。

≪参考≫

刑事訴訟法（昭和23年法律第131号）

第197条第2項

捜査については、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。

少年法（昭和23年法律第168号）

第6条の4　第3項

警察官は、調査について、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。

弁護士法（昭和24年法律第205号）

第23条の2

弁護士は、受任している事件について、所属弁護士会に対し、公務所又は公私の団体に照会して必要な事項の報告を求めることを申し出ることができる。申出があつた場合において、当該弁護士会は、その申出が適当でないと認めるときは、これを拒絶することができる。

2　弁護士会は、前項の規定による申出に基づき、公務所又は公私の団体に照会して必要な事項の

報告を求めることができる。

特定電子メールの送信の適正化等に関する法律（平成14年法律第26号）

第29条

総務大臣は、この法律の施行に必要な限度において、電気通信事業者その他の者であって、電子メールアドレス又は電気通信設備を識別するための文字、番号、記号その他の符号（特定電子メール等の受信をする者が使用する通信端末機器の映像面に表示されたもの又は特定電子メール等の送受信のために用いられたもののうち送信者に関するものに限る。）を使用する権利を付与したものから、当該権利を付与された者の氏名又は名称、住所その他の当該権利を付与された者を特定するために必要な情報の提供を求めることができる。

１２－１－４．人の生命等の保護に必要な場合

（第15条第1項の解説）

(4)「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」とは、自己又は他人の権利利益を保護するため、個人情報を第三者に提供することが必要であるものの、本人の同意を得ることが困難である場合について手当てするものである。人の生命、身体又は財産といった具体的な権利利益が侵害されるおそれが高まっており、これを保護するために個人情報の利用が必要である場合には、個人情報を第三者に提供することに一定の合理性があると考えられる。一方こうした場合であっても、本人の権利利益侵害の予防という観点からは同意を得るべきとの原則が変わるものではないことから、本人の同意を得ることが困難である場合に限って本条の規定の適用を除外するものである。したがって、人の生命、身体又は財産の保護のために、他の方法によることが十分可能である場合にまで本人の同意なき第三者への提供を認めるものではない。

なお、通信の秘密に属する事項については、この場合も通信当事者の同意なき第三者提供が許されるのは、緊急避難の要件に該当する場合等違法性阻却事由がある場合に限られる。

１２－１－５．公衆衛生の向上等に必要な場合

（第15条第1項の解説）

(5)「公衆衛生の向上又は児童の健全な育成のために、特に必要がある場合であって、本人の同意を得ることが困難なとき」とは、個人情報保護法第23条第１項第3号と同様の規定であるが、これは個人情報保護法第16条第3項第3号及び第23条第１項第3号は、疾病の予防や、治療に関する研究や、心身の発達途上にある児童の健全な育成のため、社会全体の組織的な協力により個人情報を相互に提供して活用する必要がある場合の規定であり、具体的には、疾病の予防や治療に関する研究のために、病院や医療研究機関が情報を交換する場合や、児童虐待に対応するために、学校、施設、病院、警察等がネットワークを形成する必要がある場合等が想定されている。

これらの規定が、電気通信事業者にも適用されるかについては、個別具体的に判断する必要があるが、上記の趣旨を踏まえれば、これらの規定が電気通信事業者に適用されることは基本的には想定されないと考えられる。

１２－１－６．慎重な判断

（第15条第1項の解説）

(6) なお、第1項各号に該当する場合の本人の同意なき個人情報の第三者提供については、個人情報保護の要請が特に高い電気通信事業者としては、本人の同意を得ずに第三者提供を行うことが真に必要であると慎重に判断した上で行うこととすべきである。

同意なき個人情報の第三者提供については、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（総務省）において、「個人情報保護の要請が特に高い電気通信事業者としては、本人の同意を得ずに目的外利用を行うことが真に必要であると慎重に判断した上で行うこととすべきである」とされており、事業者において、慎重な判断が求められている。

１２－２．オプトアウト

[ガイドライン　第15条]

第2項　電気通信事業者は、第三者に提供される個人情報について、本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人情報を第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人情報の項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること。

第3項　電気通信事業者は、前項第2号又は第3号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

（第15条第2項、第3項の解説）

(7) 第2項及び第3項の規定は、個人情報保護法第23条第2項及び第3項と同様の規定であり、いわゆるオプトアウトの仕組みによる第三者提供を認めたものであるが、電気通信事業者が加入者の個人情報を第三者提供する場合は、契約約款により本人の同意を得て行うことが一般的に可能である（上記(2)参照）ので、基本的には本人の同意を得て行うこととすることが望ましいと考えられる。ただし、契約約款により本人の同意を得て行う場合でも、電話帳に掲載する場合など本人の意思をできるだけ尊重すべきものについては、本人の申出により提供を停止するという扱いにすることが望ましい。

オプトアウトの仕組みにより第三者への個人情報を提供する場合には、第三者に提供するまでに、第三者提供停止の求めを受け付けられる状態にしておく必要がある。

また、第三者提供停止の求めの受付は、ガイドライン第１７条第３項の「第三者提供停止の求め」の取扱い(注)とは異なり、簡易かつ直ちに応じる必要がある。

（注）ガイドライン第17条第3項の「第三者提供の停止の求め」は、その求めがあったときは「遅滞なく調査を行うもの」とされているが、オプトアウトの仕組みに際して第三者提供停止の求めがあった場合は、求めを受け付けた以後、第三者提供に係る「同意」が取り消されたものとして扱うことになる。

１２－３．第三者に該当しないもの

［ガイドライン　第15条］

第4項　次に掲げる場合において、当該個人情報の提供を受ける者は、前3項の規定の適用については、第三者に該当しないものとする。

一　電気通信事業者が利用目的の達成に必要な範囲内において個人情報の取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人情報が提供される場合

三　個人情報を特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人情報の項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人情報の管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

１２－３－１．委託する場合

（第15条第4項の解説）

(8) 第4項第1号については、現在、民間企業等においては、顧客情報等大量の個人情報を利用するために必要となる編集・加工等の処理を他の企業に委託することが一般化しつつある。こうした取扱いを第三者提供とした場合、第1項に基づき、処理される個人情報の本人に対し個々に同意を取る必要が生じることとなり、事実上委託行為自体が不可能となるおそれがある。一方、電気通信事業者が個人情報の取扱いを委託した場合には、第12条により、適切な委託先を選定し、委託先に対し必要かつ適切な監督を行う責任が生じ、これらの責任を果たしていない結果、問題が生じた場合には委託元である電気通信事業者も責めを負うこととなる。これらの事情を勘案し、電気通信事業者が利用目的の達成に必要な範囲内で個人情報の取扱いを委託する場合には、電気通信事業者が行う取扱いの一部とみなし、委託先は第三者には該当しないこととしている。なお、一般に個人情報の処理を委託され、その成果物たる処理データを委託元に返すような場合は、そもそも第三者への提供であるとは解されない。

（注）電気通信個人情報保護推進センターにおいては、対象事業者の皆様への情報提供の一環として、「業務委託に関するＱ＆Ａ」を作成し活用いただいているところです。

１２－３－２．事業の承継があった場合

（第15条第4項の解説）

(9) 第4項第2号については、合併や分社化、営業譲渡などにより事業の承継があった場合、通常その承継資産には顧客情報等の個人情報が含まれると考えられ、必然的に個人情報が移転する。仮にこれを第三者提供として第1項及び第2項を適用した場合、移転される個人情報の本人すべてから同意を取る必要が生じ、事実上事業承継が困難になるおそれがある。一方、事業承継に伴って個人情報が移転する場合には、第5条第2項により利用目的も引き継がれることとなるため、本人との関係においては、単に取扱いの主体となる事業者の名称が変更したに過ぎず、個人情報の取扱いに伴う権利利益の侵害のおそれが増大することは考えにくい。これらの事情を勘案し、事業を承継する者は本条の対象となる第三者には該当しないこととしている。

１２－３－３．共同利用の場合

[ガイドライン第15条]

第5項　電気通信事業者は、前項第3号に規定する利用する者の利用目的又は個人情報の管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

（第15条第4項、第5項の解説）

(10) 第4項第3号及び第5項については、個人情報保護法第23条第4項第3号及び第5項と同様の規定であり、これらの規定を満たす形で特定の者との間で個人情報を共同利用することは本人の同意なく行うことができることを認めたものであるが、電気通信事業者が加入者の個人情報を共同利用する場合は、契約約款により本人の同意を得て行うことが一般的に可能である((2)参照)ので、基本的には本人の同意を得て行うこととすることが望ましいと考えられる。ただし、契約約款により本人の同意を得て行う場合でも、不払い者等情報の交換の場合のように（第27条参照）、本人の権利利益に重大な影響を及ぼす可能性がある情報を交換する場合などには、第4項第3号に掲げられている情報をあらかじめ本人に通知又は本人が容易に知り得る状態に置くなどの措置をとり、本人の権利利益を不当に侵害することのないようにすることが求められる。なお、「本人が容易に知り得る状態に置く」とは、公表が継続的に行われている状態をいい、具体的には、ホームページへの掲載、官報・新聞等への継続的な掲載、事務所の窓口等への書面の掲示・備え付け等の措置をとっていることをいう。

１２－４. 通信の秘密の保護

[ガイドライン　第15条]
第6項　電気通信事業者は、個人情報を第三者に提供するに当たっては、通信の秘密の保護に係る電気通信事業法第4条その他の関連規定を遵守するものとする。

（第15条第6項の解説）
(11) 第6項の規定は、第1項から第5項までの規定の適用により第三者提供（第4項各号の規定により提供する場合を含む。）が認められる場合であっても、個人情報が通信の秘密にも該当する場合には、通信当事者の同意なき第三者提供（同上）は違法性阻却事由がある場合を除き許されないことについて念のため確認する趣旨の規定である。

≪参考≫
電気通信事業法（昭和59年12月25日法律第86号）
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。
2　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

１３．個人情報に関する事項の公表等（ガイドライン第１６条）

[ガイドライン]

第16条　電気通信事業者は、個人情報に関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くものとする。

一　当該電気通信事業者の氏名又は名称

二　すべての個人情報の利用目的（第８条第４項第１号から第３号までに該当する場合を除く。）

三　次項又は次条第１項若しくは第３項の規定による求めに応じる手続（第20条第２項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四　当該電気通信事業者が行う個人情報の取扱いに関する苦情の申出先

五　当該電気通信事業者が認定個人情報保護団体（個人情報の保護に関する法律第37条第１項の認定を受けた者をいう。以下同じ。）の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

（第16条第1項の解説）

(1) 第１項各号に掲げる事項は、開示等の求めを本人が行う上での実効性を確保し、また、電気通信事業者による個人情報の取扱いを公平性の確保を図ろうとする観点から必要不可欠な事項を掲げているものである。

(2)「本人の知り得る状態」とは、本人が知ろうとすれば知ることができる状態をいい、ホームページへの掲載、パンフレットの配布、書面の掲示・備付け等の措置をとっていることをいい、本人の求めに応じて遅滞なく回答する場合を含む。

なお、「本人の知り得る状態」とは、第8条等の規定における「公表」の概念とは一部、異なり、その時点で本人が知ろうと思えば知り得ることを指す。したがって、数年前に官報や新聞に一度掲載されたということは、「公表」とは言えるが、「本人の知り得る状態」とは必ずしも言えない。

また、「本人の知り得る状態に置くものとする」とは、その時点において正確な情報を正確な状態で本人の知り得る状態に置くことをいうものであり、内容に変更があった場合には、必ずその内容を変更し、常にその時点での正確な内容を「本人の知り得る状態」におくことが要請される。

本条において、「本人の知り得る状態」に「本人の求めに応じて遅滞なく回答する場合を含む」こととしているのは、電気通信事業者の規模や個人情報の取扱いの態様等からみて、一律に本人の知り得る状態に置くこととすることは、負担が過重となる場合があることを考慮したものである。

ただし、非常に問い合わせが多いことが予想される電気通信事業者においては、ホームページへの掲載、パンフレットの配布、書面の掲示・備付け等の措置の方が、個別の求めへの回答より負担が軽い場合もある。また、当該電気通信事業者が電子商取引を行っているかどうかと

いった事業形態によっても、措置の形態の妥当性（ホームページへの掲載、パンフレットの配布、書面の掲示・備付け等の措置のうちいずれの措置が妥当か等）が変わってくることが考えられる。したがって、本条については、「本人の知り得る状態に置かなければならない」方法を限定するものではないが、当該電気通信事業者が、その事業形態や個人情報の取扱いの態様等を踏まえ、できるだけ本人が容易に知り得るような状態としていくことが望ましいと考えられる。

(3) 第１項第２号については、個人情報に関し、その取扱いについて、利用目的による制限を実効あらしめるようにするために、括弧書きの場合を除き、すべての個人情報の利用目的を明らかにすることを求めているものである。利用目的に第三者提供が含まれる場合には、その旨も明らかにする必要がある。

(4) 第１項第３号については、開示等の求めに応じる手続は、第１９条の規定等に基づき電気通信事業者が個別に定めることとなるが、求めを受け付ける場所、方法、本人確認の方法等の手続について定めた場合には、本条の規定により本人の知り得る状態に置く必要がある。

　また、本人の求めに応じる際に第20条の規定に基づき手数料を徴収する場合、手数料の額が事前に明らかにされていることが本人の求めの実効性を確保する上で必要であり、括弧書きの規定はその旨を確認的に規定したものである。

対象事業者は認定個人情報保護団体として、電気通信個人情報保護推進センターを苦情の申出先として公表等する必要がある。

＜記載例＞

認定個人情報保護団体の名称

「（財） 日本データ通信協会」

申出先の名称等（注）

「電気通信個人情報保護推進センター」

電話：０３－５９０７－３８０３

Ｅ－ｍａｉｌ： privacy@dekyo.or.jp

（注）申出先の名称等は次のようにリンクを張ることにより簡略化することも可能である。
「電気通信個人情報保護推進センター（URL:http://www.dekyo.or.jp/kojinjyoho/）」

[ガイドライン第16条]
第2項　電気通信事業者は、本人から、当該本人が識別される個人情報の利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知するものとする。ただし、次の各号のいずれかに該当する場合は、この限りでない。
一　前項の規定により当該本人が識別される個人情報の利用目的が明らかな場合
二　第8条第4項第1号から第3号までに該当する場合

（第16条第2項の解説）
(5) 第2項は、電気通信事業者が、本人から、当該本人が識別される個人情報の利用目的の通知を求められたときは、本人に対し、その利用目的を通知するものとすることを規定するものである。

[ガイドライン第16条]
第3項　電気通信事業者は、前項の規定に基づき求められた個人情報の利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知するものとする。

１４．個人情報の開示及び訂正等（ガイドライン第１７条）

１４－１．開示の求め

[ガイドライン]

第17条　電気通信事業者は、本人から、当該本人が識別される個人情報の開示（当該本人が識別される個人情報が存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）により、遅滞なく、当該個人情報を開示するものとする。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部について開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　当該電気通信事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

三　他の法令に違反することとなる場合

第2項　電気通信事業者は、前項の規定に基づき求められた個人情報の全部又は一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知するものとする。

（第17条第1項の解説）

(1)　第1項は、電気通信事業者は、個人情報に関し、本人の求めにより開示するものとすることを規定するものである。「開示」とは、開示を求められた個人情報の存否を含めてその内容を知らせることを指す。なお、電気通信事業者が開示すべき個人情報は、当該電気通信事業者が開示の権限を有している個人情報である。

(2)「遅滞なく」とは、事情の許す限り最も速やかにという意味であり、正当な又は合理的な理由に基づく遅滞は許されると解されている。したがって、例えば、同一主体からの大量の開示請求があった場合には開示が遅れてもやむを得ない。

(3)「本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合」とは、例えば、本人に関する情報の中に第三者の情報が含まれており、これを開示することが当該第三者の不利益となるような場合などが考えられる。

また、個人情報保護法施行令第3条第1項各号に該当するような場合、すなわち

1)　当該個人情報の存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

2)　当該個人情報の存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

3)　当該個人情報の存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

4)　当該個人情報の存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるものも、これに該当することとなると考えられる。

(4)「業務の適正な実施に著しい支障を及ぼすおそれがあるとき」とは、例えば、開示の対象が特定されていない場合や個人データに該当しない個人データベース等を構成していない個人情報（Webサーバに一時的に保存されているクッキー情報である個人情報等）の開示が求められた場合などこれに応じて開示を行うことが電気通信事業者に過大な負担となるような場合や電気通信事業者において独自に付加した信用評価等の開示が求められた場合をいう。

本人から、ガイドライン第１７条第１項の規定に基づき、当該個人が識別される個人情報の開示を求められたときは、ガイドライン第１７条第１項各号に該当する場合を除き、遅滞なく当該個人情報を開示しなければならない。また、「１６．開示等の求めに応じる手続き」に示すように、電気通信事業者は、開示の求めを受け付ける方法をあらかじめ定めることができる。もっとも、電気通信事業者がサービスを提供するにあたっては、失念したＩＤやパスワード、新サービスへの加入に際しての工事日や開通日といった事項に関してユーザー本人からの問い合わせが数多く寄せられるが、本人にガイドライン第１７条第１項の規定に基づく開示の求めを行う意思がなく、これらの事項について単なる問い合わせを行っている場合には、ガイドライン第１７条第１項の規定に基づく求めとは考えられないことから、本人からの問い合わせである場合にはコールセンター等において適宜の方法により回答することとなると考えられる。

○（好ましい事例）

事例１４－１　電気通信サービスの変更申込書は２ヶ月で、廃棄することになっており、法の「保有個人データ」に該当しないが、保存期間中は、開示の求めに応じることとしている。

×（好ましくない事例）

事例１４－２　本人から個人情報の開示を求められたにもかかわらず、長期間放置している。

１４－２．訂正等の求め

〔ガイドライン第17条〕

第3項　電気通信事業者は、本人から自己に関する個人情報の訂正等（訂正、追加若しくは削除又は利用の停止若しくは第三者への提供の停止をいう。以下同じ。）を求められたときは、遅滞なく調査を行うものとする。この場合においてその求めに係る個人情報の内容が事実でないとき、保存期間を経過しているときその他当該個人情報の取扱いが適正でないと認められるときは、遅滞なく訂正等を行うものとする。

第4項　電気通信事業者は、前項の規定に基づき求められた個人情報の内容の全部若しくは一部について当該個人情報の訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）の通知を行うものとする。

（第17条第3項の解説）

(6) 訂正等を行うべきなのは、当該個人情報の内容が事実でない場合のほか、当該電気通信事業者が当該個人情報を第10条の規定に違反して保存期間経過後も消去しない場合、第6条の規定に違反して目的外に利用している場合、第15条の規定に違反して本人の同意なく第三者に提供している場合など本ガイドラインに違反した取扱いを行っている場合である。

(7) 本ガイドラインに違反した取扱いを行っている場合には、本ガイドラインに違反している取扱いを是正すれば足り、必ずしも当該個人情報のすべての取扱いをやめる必要はない（例えば、第6条の規定に違反して目的外に利用している場合は目的外利用を停止すればよく、利用目的の範囲内の利用まで停止する必要はない。）。なお、「第三者への提供の停止」とは、新たな提供を停止することを意味し、既に第三者に提供された個人情報を回収することは含まれない。

本人から、ガイドライン第１７条第３項の規定に基づき、自己に関する個人情報の訂正、追加若しくは削除又は利用の停止若しくは第三者への提供の停止を求められたときは、遅滞なく調査を行い、ガイドラインに違反した取扱いを行っていることが判明した場合には、その違反を是正し、是正の内容を遅滞なく本人に通知しなければならない。また、ガイドラインに違反した取扱いを行っているとは認められない場合には、その旨を本人に通知しなければならない。

なお、ガイドライン第１７条３項に基づく個人情報の第三者への提供の停止の取扱いは本ガイドラインに違反した第三者提供に関するものであり、ガイドライン第１５条第２項にのっとったオプトアウトの場合の第三者提供の停止の求めの取扱いとは異なることに注意する必要がある。

×（好ましくない事例）

事例１４－３　本人から個人情報の削除を求められ、調査の結果、その者の個人情報を目的外に利用していたことが判明したにもかかわらず、何の措置もとらなかった。

１５．理由の説明（ガイドライン第１８条）

[ガイドライン]

第18条　電気通信事業者は、第16条第3項又は前条第2項若しくは第4項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めるものとする。

（第18条の解説）

本条は、電気通信事業者が、本人からの開示等の求めに対して、第16条第3項又は第17条第2項若しくは第4項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めるものとすることを規定したものである。なお、本人の求めに応じた措置をとる場合は、本人の求めによることがその措置をとる理由であり、理由が自明であることから、理由を説明することとはしていない。

○（好ましい事例）

事例１５－１　本人から個人情報の開示を求められた場合であって、その求めに係る個人情報に第三者の通信の秘密に属する情報が含まれている場合に、本人に対して開示しない旨理由を付して知らせる。

１６．開示等の求めに応じる手続（ガイドライン第１９条）

１６−１．受付ける方法

[ガイドライン]

第19条　電気通信事業者は、第16条第2項又は第17条第1項若しくは第3項の規定による求め（以下この条において「開示等の求め」という。）に関し、その求めを受け付ける方法として次の各号に掲げるものを定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行うものとする。

一　開示等の求めの申出先

二　開示等の求めに際して提出すべき書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

三　開示等の求めをする者が本人又は第3項に規定する代理人であることの確認の方法

四　次条第1項の手数料の徴収方法

（第19条第1項の解説）

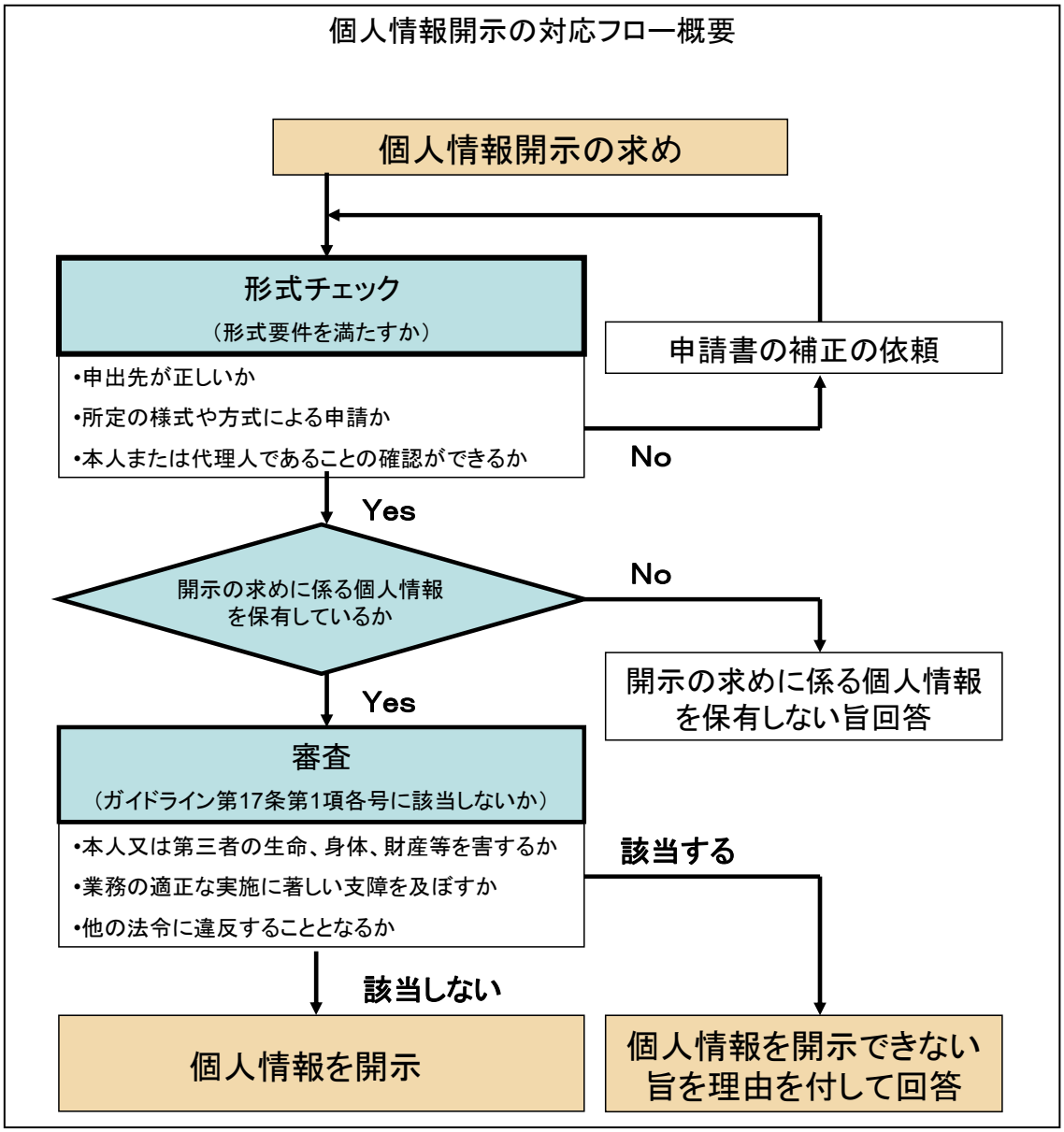
(1)「求めを受け付ける方法」とは、求めを受け付けるための申請書の様式、窓口の特定、郵送等による受付を認めるかどうかといったことを想定している。第1項については、電気通信事業者は必ずしも申請書の様式や窓口の特定等を定める必要があるものではなく、定めない場合には自由な申請を認めることとなる。一方、電気通信事業者が同項の規定に基づき申請書の様式等の求めを受け付ける方法を定めたときは、本人は、当該方法に従って、開示等の求めを行う必要がある。

１６－１－１．受付方法

ガイドライン第１９条が対象とする手続は、利用目的の通知、個人情報の開示及び訂正等であり、電気通信事業者はそれぞれの求めの受付方法をあらかじめ定めることができる。また、求めを受け付ける方法としては、申請書等の直接窓口への提出や電子メール、ファックス若しくは郵便等による送信などがあり、複数の手段で受け付けることが望まれる。

① 開示の求めについては、あらかじめ電気通信事業者が定めた受付方法に従っているかどうかの形式をチェックすることとなる（開示の求めの申出先、申請書の様式、その他の求めの方式及び本人又は代理人であることの確認。なお、本人又は代理人であることの確認については「１６－１－２．本人又は代理人の確認方法」参照のこと）。ここで不備があれば、開示を求めた者（以下「申請者」という。）に連絡し、申請書の補正を求めることとなる。申請者が補正の求めに応じない場合は、開示の求めには応じられない旨を回答することとなる。ついで、電気通信事業者が開示の求めに係る個人情報を保有しているか否かを調査し、保有していない場合にはその旨を本人に回答しなければならない。保有している場合には、当該情報を開示することにより、ガイドライン第１７条第１項各号に該当するかどうかを審査し、該当しない場合には本人に開示し、該当する場合には個人情報を開示できない旨理由を付して回答することとなる。

開示の求めがあった場合の対応フローの概要を次に示す。



② 訂正等の求めがあった場合についても、電気通信事業者が訂正等の求めに係る情報を保有しているか否かを調査するところまでは、開示の求めがあった場合と同様である。開示の求めと訂正等の求めが大きく相違する点は、開示の求めの場合には申請者がその理由を述べる必要がないのに対して、訂正等の求めの場合は申請者がその理由を明らかにする必要がある点である。訂正等の求めに応ずる必要があるのは、訂正等の求めについて申請者の申出を受けて個人情報及びその取扱いについて調査し、その結果、当該個人情報の内容が事実でないこと、当該個人情報をガイドライン第１０条の規定に違反して保存期間経過後も消去していないこと、第６条の規定に違反して目的外に利用していること、

第１５条の規定に違反して本人の同意なく第三者に提供していることなどガイドラインに違反した取扱いを行っていると認められた場合である。ガイドラインに違反した取扱いを行っていると認められた場合は、速やかに訂正等を行うとともに、訂正等をした旨を本人に回答しなければならない。この場合において、必ずしも本人から求められた措置を講ずる必要はなく、ガイドラインに違反した取扱いを是正する措置を講ずることで足りるものであり、この場合も、その旨の理由を付して本人に回答しなければならない。また、ガイドラインに違反した取扱いを行っていると認められない場合には、その旨を、理由を付して本人に回答しなければならない。

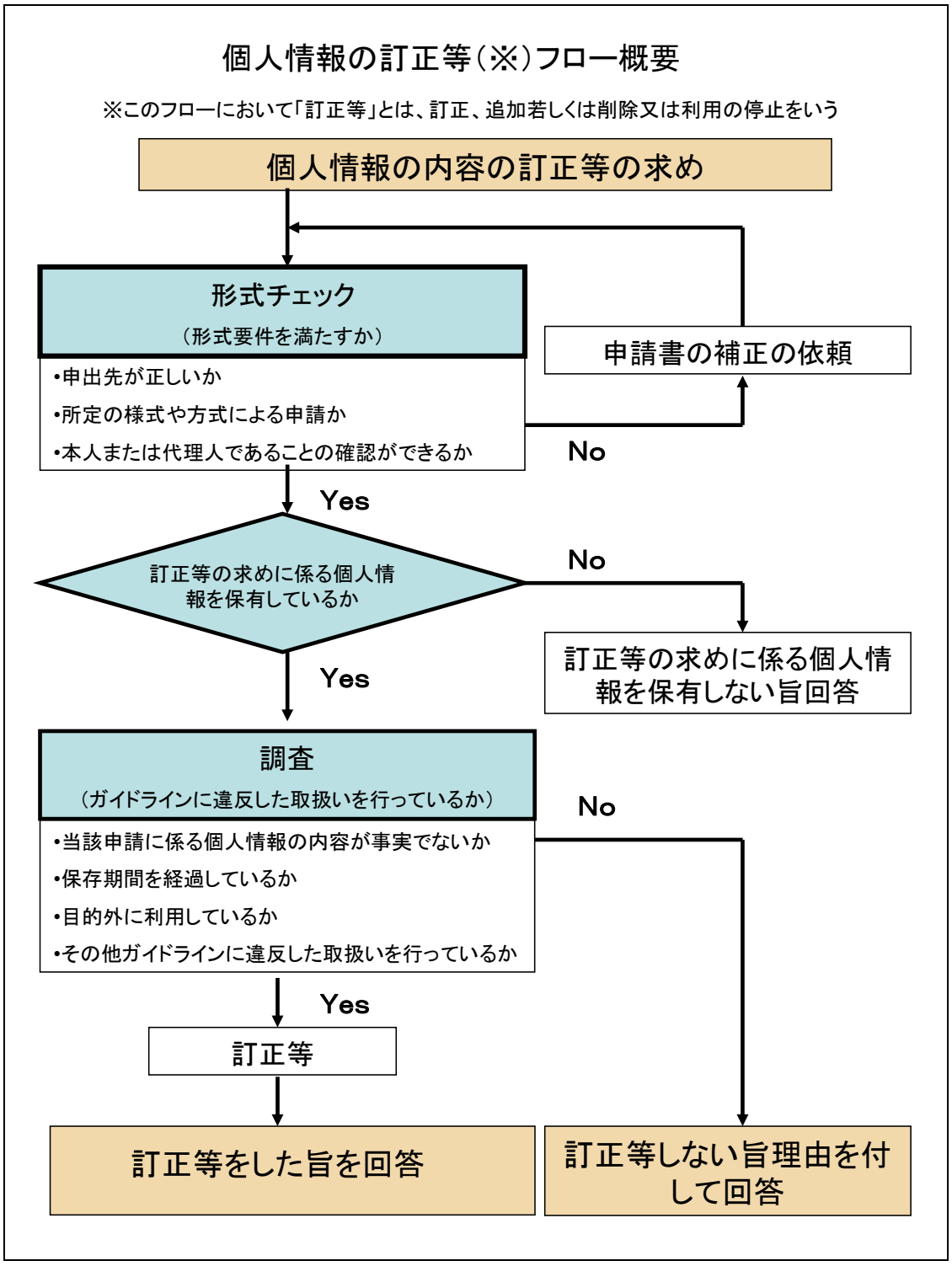
ただし、第三者提供停止の求めがなされた理由として、個人情報の漏えい等重大事故が発生している場合も想定されることから、第三者提供の停止の求めがあった場合には、形式要件を満たすか否かにこだわることなく、速やかに事実関係の確認を行うべきである。

また、オプトアウト方式による第三者提供停止の求めの受付とも異なる取扱いである。

×（好ましくない事例）

事例１６－１　個人情報が第三者に漏えいしているとの申告が電話であったが、具体的な漏えいの事実を聞くこともなく、所定の第三者提供停止申請書及び本人確認書類を提出するよう求めた。

訂正等の求めがあった場合の対応フローの概要を次に示す。



電気通信事業者が、個人情報の利用目的の通知、開示、訂正・追加・削除、利用停止・消去及び第三者提供停止に係る申請書並びにこれらの申請書に対す

る回答書の記載例を参考資料１の例６から例１５に示す。これらは、電気通信事業者がそれぞれの業務の内容や事業の形態に応じた様式を作成するにあたっての参考として示すものである。

１６－１－２．本人又は代理人の確認方法

電気通信事業者が、本人確認手続を十分に行わない状態で安易に開示等の求めに応じ、その結果として本人になりすました第三者に対して誤って開示を行うと、本人の権利利益が害され、また個人情報の漏えいと判断され得ることとなる。こうした事態の発生を回避するため、開示等を求める者が本人又は代理人であることを確認する方法を定めることとするべきであり、具体的には、次のような確認方法が考えられる。

①　申請者が本人である場合

申請者に対して、開示の求めの受付方法に応じて次の書類の提示又は提出を求める。

開示等の求めの申出先に開示等の申請書を直接提出する場合	開示等の求めの申出先に開示等の申請書を郵送等する場合
本人であることを確認するに足りる書類（以下「本人確認書類」という）いずれか一つ（開示等の申請書に記載されている開示等を求めるものの氏名及び住所と同一の氏名及び住所が記載されている運転免許証、健康保険の被保険者証、外国人登録証明書、住民基本台帳カード又は旅券等）	１　左に掲げる書類のいずれか一つのコピー ２　その者の住民票の写し又は外国人登録原票の写し 例：運転免許証のコピー及び住民票の写し

②　申請者が本人の代理人である場合

ガイドライン第１９条第３項においては、未成年者又は成年被後見人の法定代理人、又は開示等の求めをすることにつき本人が委任した代理人が開示等の求めをすることができることとされている。それぞれの代理人に対して、開示の求めの受付方法に応じて次の書類の提示又は提出を求める。なお、法定代理人が本人の具体的な委任によらず開示等の求めをしてきた場合などに、本人の通信の秘密に属する事項についての情報（例えば利用明細など）を開示等すると、電気通信事業法第１７９条第２項に該当し得るので、電気通信事業者においては、開示等する情報の中に通信の秘密に属する情報が含まれないことを十分に確認する必要がある。

代理人	開示等の求めの申出先に開示等の申請書を直接提出する場合	開示等の求めの申出先に開示等の申請書を郵送等する場合
法定代理人	1　戸籍謄本、戸籍抄本、家庭裁判所の証明書、登記事項証明書等その資格を証明する書類（開示等の求めをする日前30日以内に作成されたものに限る） 2　代理人自身の本人確認書類	1　左記1の書類 2　左記2の書類のコピー 3　代理人自身の住民票の写し又は外国人登録原票の写し
本人が委任した代理人	1　委任状 2　当外委任状を本人が作成したことを確認できる書類（委任状に押された本人の実印の印鑑証明書等） 3　代理人自身の本人確認書類 4　本人の本人確認書類	1　左記1の書類 2　左記2の書類 3　左記3の書類のコピー 4　代理人自身の住民票の写し又は外国人登録原票の写し 5　左記4の書類のコピー

（注1）この表においては、代理人からの開示等の求めがあった場合、本人の本人確認書類の提示又は提出を求めているが、各電気通信事業者の判断により、本人の本人確認書類の提示又は提出を省略することも考えられる。

（注2）顔写真が添付されていない確認書類による本人確認の場合には、なりすまし防止のため、特に注意する必要がある。

（注3）本人が委任したことを証するため、印鑑登録された印鑑の押印とその印鑑証明書の添付を求めることも可能であるが、印鑑登録は15歳未満の未成年や成年被後見人には認められていないことに注意する必要がある。

電気通信事業者が、代理人による開示等の申請を受け付ける場合に提出を求める委任状の記載例を参考資料１の例１６に示す。これは電気通信事業者が、利用者の便宜を図るため委任状の様式を作成するにあたっての参考として示すものである。

１６－２．個人情報の特定

[ガイドライン　第19条]
第2項　電気通信事業者は、本人に対し、開示等の求めに関し、その対象となる個人情報を特定するに足りる事項の提示を求めることができる。この場合において、電気通信事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該個人情報の特定に資する情報の提供その他本人の利便を考慮した適切な措置をとるものとする。

（第19条第2項の解説）
(2)「対象となる個人情報を特定するに足りる事項の提示を求めることができる」とは、電気通信事業者が事業部門や営業所ごとに個人情報を保有している場合や、取得年月日別に個人情報を保有している場合等において、電気通信事業者は、開示等の求めについて、具体的にどの区分の個人情報を対象とするものなのかについて、特定を求めることができることとするものである。また、「特定に資する情報の提供その他本人の利便を考慮した適切な措置をとる」とは、電気通信事業者が、本人に対し、対象となる個人情報を特定するに足りる事項の提示を求める場合においては、個人情報の区分を本人の知り得る状態に置くこと等により、本人が容易に特定し得るような措置をとる必要があることを規定したものである。

ガイドライン第１７条第１項又は第３項の規定による開示又は訂正等の対象となるのは、電気通信事業者が保有し、かつ開示又は訂正等の権限を有する情報であって、個人を識別することのできる情報すべてである（ただし、ガイドライン第１７条第１項各号の場合を除く）。特定に資する情報の提供その他本人の利便を考慮した適切な措置の一環として開示又は訂正等の対象となる個人情報の項目を示すことも考えられるが、あらかじめ示した項目に入っていないことを理由に開示又は訂正等を拒むことは許されないものである。

○（好ましい事例）

事例１６－２　本人から「貴社が保有する私に関するすべての個人情報を開示して欲しい」との求めがあった場合に、本人に対し開示の対象となる個人情報を特定するに足りる事項の提示を求める。

×（好ましくない事例）

事例１６－３　保有する個人情報の一部のみを開示に応ずる個人情報として示し、それ以外の個人情報の開示が求められた場合、ガイドライン第１７条第１項各号の場合にあたらないにもかかわらず、あらかじめ示した開示対象でないとして開示を行わない。
（例）当社が保有するお客様の個人情報のうち、当社が開示に応ずる個人情報は次のと

おりです。

氏名、住所、性別、ＩＤ番号、メールアドレス、電話番号（固定・携帯）

１６－３．代理人による求め

[ガイドライン第19条]
第3項　開示等の求めは、次に掲げる代理人によってすることができる。ただし、第17条第1項の規定による開示の求めについては、本人の具体的な委任によらない代理人に開示することにより、本人の通信の秘密を侵害する場合等同項各号のいずれかに該当する場合はこの限りでない。
一　未成年者又は成年被後見人の法定代理人
二　開示等の求めをすることにつき本人が委任した代理人

（第19条第3項の解説）
(3) 開示等の求めに関しては、本人が遠隔地にいる場合や傷病の場合等において、本人の便宜の観点から、代理人による求めを認める必要があるため、第3項各号に掲げる代理人によって開示等の求めをすることができることとしている。なお、同項ただし書は、本人の具体的な委任によらない代理人に利用明細を開示する等本人の通信の秘密を侵害することとなる場合や代理人による開示の求めを認めることが本人と利益相反となるおそれがある場合等第17条第1項各号のいずれかに該当する場合には、代理人による求めは認められないことを念のため確認的に規定したものである。

電気通信事業に従事する者が、単に法定代理人であるという理由だけで通信の秘密に属する情報を当該法定代理人に開示してしまうと、電気通信事業法第１７９条第１項にいう「通信の秘密を侵した」に該当し、同条第２項の規定により刑罰を科されうるので注意を要する。

×（好ましくない事例）

事例１６－４　本人から具体的な委任を受けていない法定代理人から、本人の利用明細や通信履歴の開示の求めがあった場合に、これに応じてしまい、本人の通信の秘密が侵害された。

１６－４　過重な負担

［ガイドライン　第19条］
第4項　電気通信事業者は、前3項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮するものとする。

（第19条第4項の解説）
(4) 電気通信事業者は、第1項から第3項までの規定に基づき開示等の求めに応じる手続をそれぞれ定めることとなるが、本人に過重な負担を課するような手続を定めた場合、事実上開示等の求めを制限することとなるおそれがあることから、第4項の規定を置いたものである。「本人に過重な負担を課する」手続は、個人情報の性質又は利用方法により、ある程度異なるものと考えられるが、必要以上に煩雑な書類を書かせることや、求めを受け付ける窓口を他の業務を行う拠点とは別にいたずらに不便な場所に限定すること等はこれに該当するものと考えられる。

１７．手数料（ガイドライン第２０条）

[ガイドライン]

第20条　電気通信事業者は、第16条第2項の規定による利用目的の通知又は第17条第1項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。

第2項　電気通信事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めるものとする。

（第20条の解説）

本条は、電気通信事業者が第16条第2項の規定による利用目的の通知又は第17条第1項の規定による開示を求められたときは、その実施に関し、手数料を徴収することができること、また、手数料を徴収する場合は、実費を勘案して合理的に認められる範囲内において、その手数料の額を定めるものとすることを規定するものである。

ガイドライン第２０条において規定されている手数料は、利用目的の通知及び個人情報の開示の求めに関してであり、訂正等を求められた場合には、手数料を徴収することはできないものである。なお、不開示の場合であっても、手数料を徴収することができる。

開示や利用目的の通知については、本人から求められれば事業者としてはそれに応じざるを得ないことから、実費を勘案して合理的に認められる範囲において手数料を徴収することが法により認められているが、合理的な範囲を超えて手数料の額を設定した場合には、法第３４条第１項の規定による総務大臣の勧告の対象となりうるものである。具体的な手数料の額の算定に当たり、費用の内訳としては次のようなものが考えられる。

①受付事務にかかる費用、②本人確認の手続にかかる費用、③検索作業にかかる費用、④開示等の求めに応ずるか否かの審査にかかる費用、⑤回答書等の作成にかかる費用、⑥回答書等の送付料、（ただし、②、③及び④は開示の求めの場合に限られる）

費用内訳	具体的な作業	費用
①受付事務にかかる費用	記載事項の確認等	作業にかかる人件費
②本人確認の手続にかかる費用	申請書の記載事項と本人であることを示す書類を照合	作業にかかる人件費
③検索作業にかかる費用	データベース検索や倉庫・書庫等の探索	作業にかかる人件費、データベースの稼働にかかる経費

④開示等の求めに応ずるか否かの審査にかかる費用	ガイドライン第16条第2項第1号若しくは第2号、又は第17条第1項各号に該当するか否かの審査	作業にかかる人件費
⑤回答書等の作成のかかる費用	回答書の作成	作業にかかる人件費、用紙代等の消耗品費
⑥回答書等の送付にかかる費用	郵送、ファクシミリによる送付など	郵送費、通信費

電気通信事業者は、これらの項目を勘案し合理的な範囲内で手数料を設定するものとする。なお、個人情報を開示するに当たり、回答書等を郵送する場合は、簡易書留、書留、本人限定受取郵便など本人に確実に届く手段を用いるべきであり、この場合は実際にかかる郵送費を手数料に含めることができる。

手数料の支払い方法としては、定額小為替証書、切手、現金書留、クレジットカード、口座振込などが考えられるところであり、開示等の求めの受付方法に応じた支払い方法を定めることとなる（例えば、開示等の求めの受付方法が「郵送」である場合には、定額小為替証書、切手、現金書留、クレジットカードのうちいずれか、又は複数を認めることになると考えられる）。

なお、手数料の額、支払い方法を定めた場合もあらかじめこれらを公表しておくか、本人の求めに応じて遅滞なく回答する必要がある。（ガイドライン第１６条第１項第３号）

また、一般的なケースに関する合理的な手数料を設定するとともに、例外的な一部の個人情報を開示するために、データベースの検索、倉庫・書庫の探索等に多大な費用が発生することが予想され、そのコストを勘案した場合の手数料が相当高額になる場合など例外的なケースについては、その都度見積を提示する旨を明記することも可能である。

×（好ましくない事例）

事例１７－１　手数料の額が、実質的に開示の求めを拒むのと同等と見なされる法外な額に設定されている場合。

事例１７－２　支店があるにもかかわらず、本店のみで開示申請を受け付ける。

１８．苦情の処理（ガイドライン第２１条）

１８－１．　適切かつ迅速な処理

[ガイドライン]
第21条　電気通信事業者は、個人情報の利用、提供、開示又は訂正等に関する苦情その他の個人情報の取扱いに関する苦情を適切かつ迅速に処理するものとする。

１８－１－１．適切かつ迅速な処理

（第21条第1項の解説）
(1) 本条は、電気通信事業者は、個人情報の取扱いに関する苦情について、適切かつ迅速に処理するものとすることを規定したものである。

電気通信事業者が利用者から個人情報の取扱いに関する苦情を受けた場合、これに対して責任をもって適切に対処することが、電気通信事業者の個人情報の取扱いに対する利用者の不平・不満をスムーズに解決することにつながり、電気通信事業者の個人情報の取扱いについての信頼を得る上で重要であると考えられる。

法及びガイドラインでは個人情報取扱事業者は苦情の適切かつ迅速な処理に努めるものとされており、電気通信事業法第２７条においても利用者からの苦情及び問合せについては適切かつ迅速に処理するものとされている。

なお、苦情処理にあたっては、電気通信事業法の消費者保護ルールに関するガイドライン(注)の第３章「苦情等の処理（事業法２７条）関係」も参照されたい。

（注）総務省ホームページで公開されている
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/syohi/pdf/090708_1.pdf

１８－１－２．苦情

（第21条第1項の解説）
(2)「個人情報の取扱いに関する苦情」とは、個人情報の取扱いに関する不平不満をいう。

ここでいう苦情とは、ガイドラインにあるように『個人情報の取扱いに関する不平不満』を指し、具体的には次のような苦情が寄せられることが考えられる。

① 個人情報を目的外に取得又は利用している（ガイドライン第４条、第５、第６条関連）
② 個人情報を不適正な方法により取得している（ガイドライン第７条関連）
③ 個人情報の利用目的が通知又は公表されていない（ガイドライン第８条関連）
④ 個人情報が正確でない、又は最新のものでない（ガイドライン第９条関連）
⑤ 利用目的を達成した又は保存期間を経過したにもかかわらず個人情報を保有し続けている（ガイドライン第１０条関連）
⑥ 個人情報が漏えいしている（ガイドライン第１１条、第１２条関連）
⑦ 個人情報を本人の同意なしに、第三者に提供している（ガイドライン第１５条関連）
⑧ 個人情報の開示等を求めたにもかかわらず、速やかに開示等されない（ガイドライン第１７条関連）
⑨ 開示の求めの方法が分かりにくい（ガイドライン第１９条関連）
⑩ 開示に要する手数料が高い（ガイドライン第２０条関連）　等

１８－１－３．事業者としての苦情処理上の留意点

（第21条第1項の解説）

(3) 苦情を適切かつ迅速に処理しているか否かについては、電気通信事業者によって提供する電気通信サービスの内容、利用者層、利用者数等が様々であること、また苦情の内容も様々であることから、「適切かつ迅速な処理」の具体的な内容をすべての電気通信事業者等について一律に定めることは困難であり、個別具体的に判断する必要があるが、少なくとも、以下の場合には、適切かつ迅速に処理を行っているとはいえないと考えられる。

1) 苦情に対する対応窓口を設けていない場合

2) 苦情に対する対応窓口が設けられていても、その連絡先や受付時間等を一般に明らかにしていない場合

3) 苦情に対する対応窓口が明らかにされていても、実際にはその対応窓口がほとんど利用できないような場合（例えば、電話窓口に頻繁に電話しても繋がらない場合やメール相談窓口にメールで繰り返し相談しても連絡がない場合）

一方、本条は、無理な注文をつけてくる場合その他のいわば行きすぎた苦情についてまで対応することを求めるものではなく、このような場合に要求を拒む等しても本条に違反することにはならない。

電気通信事業者は、利用者から苦情の申出があった場合には、おおむね次のような対応をすることが望ましい。

① 可能な範囲で本人の確認を行う。

② その苦情の内容を正しく理解する。

③ 調査など事実関係の把握に時間が必要と判断した場合には、妥当と思われる調査の方法及び回答に要する期間を提示し、処理の在り方について利用者の了解を得る。

④ 利用者に調査の結果や当該電気通信事業者としての見解を速やかに回答する。

⑤ 事実関係を調査した結果、当該電気通信事業者の個人情報の取扱いに問題があったことが判明した場合には、当該問題点を是正し、その旨を利用者にもお知らせする。

○（好ましい事例）

事例１８－１　夜間に個人情報漏えいに関する苦情の電話があったが、事務問合せ窓口での回答では納得してもらえなかったので、翌朝改めて、苦情受付窓口から電話を差し上げることを約束し、了承された。

クレーム内容によっては、関係各部門（法務担当、弁護士など）への確認をしたうえで、迅速に対応を行う。

事例１８－２　苦情対応においては、必ず事実確認を行ったうえで、回答する。

×（好ましくない事例）

事例１８－３

① 夜間に「貴社から自分の個人情報が漏えいしたのではないか」との苦情が入り、「夜なので分かる者がいない。後日連絡する。」と回答したにもかかわらず放置した。

② 苦情に対して、正当な理由なく、何ら回答をしないで長期間放置する。

③ 継続的な対応が必要とされる場合に、十分な引き継ぎがなされないまま担当者が替わってしまい、適切な対応がなされていない。

④ 苦情をたらい回しにする。

⑤ 同一の苦情に対する回答の内容に一貫性がない。

⑥ 調査や確認等を１週間程度で終えることができる問い合わせ内容に対して、正当な理由なく、１ヶ月以上の期間をかける。

１８－１－４．行きすぎた苦情への対応

苦情の内容が具体的でない場合や、事実無根であることが明らかである場合などには、申出者からの要求を拒むこともできる。

この場合、電気通信事業者において対応できない理由を申出者に分かりやすく説明することが必要である。

○（好ましい事例）

事例１８－４　「貴社が提供するコンテンツに会員登録をした後、急に迷惑メールがくるようになった。貴社から個人情報が漏えいしたのではないか、調べて報告してほしい。」との電子メールが届いた。事実関係を調査した結果、個人情報漏えいの事実はなかったので、申出者にその旨を説明するとともに、不必要に迷惑メールが届いて困るのであれば、メールアドレスを変更することを案内した。

事例１８－５　「以前、貴社のアンケートに答えたことがあるが、その時に登録した個人情報を開示してほしい」との問合せがあったが、アンケートの時期や内容が分からないと、開示の対象となる個人情報を特定することは無理であることを申出者に連絡し、了解を得た。

×（好ましくない事例）

事例１８－６　申出者からの苦情の内容が具体的でないため、回答する必要はないと判断し、放置した。

１８－２．体制の整備

[ガイドライン第21条]
第2項　電気通信事業者は、前項の目的を達成するために必要な体制を整備するものとする。

「必要な体制を整備する」とは、個人情報の取扱いに関する苦情についての専任の受付対応窓口を設けることを求めるものではないが、利用者にとって個人情報の取扱いについての苦情の申出先を明らかにすることは必要である。

苦情の受付手段としては、電話、電子メール、書面の郵送などが考えられるが、各電気通信事業者が提供する電気通信サービスの内容、利用者層、利用者数などに応じて、適切かつ迅速に処理できる方法を採用する必要がある。また、電話により苦情を受け付けることとする場合には、平日は、できるだけ長時間受け付ける体制にしておくことが望まれる。

これらの情報は自社ホームページ、パンフレットなど適宜の方法により分かりやすく表示しておくべきである。

×（好ましくない事例）

事例１８－７
① 苦情に対する対応窓口を設けていない。
② 苦情に対する対応窓口が設けられていても、その連絡先や受付時間等を一般に明らかにしていない。
③ 苦情に対する対応窓口が明らかにされていても、実際には対応窓口がほとんど利用できない（例えば、電話窓口に頻繁に電話しても繋がらない場合やメール相談窓口にメールで繰り返し相談しても連絡がない）

１８－３．認定個人情報保護団体がかかわる場合の苦情対応

個人情報の取扱いについての苦情は電気通信事業者自身の取組により解決されることが基本であるが、例えば次のような場合には、電気通信個人情報保護推進センター、各種消費者相談窓口、総務省電気通信消費者相談センターなどに相談が寄せられることとなると考えられる。

① 利用者が電気通信事業者の苦情対応窓口の対応に満足できなかった場合

② 利用者が電気通信事業者に不信を持ち苦情対応窓口とは接触したくない場合

電気通信個人情報保護推進センターは、対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知して迅速な解決を求める。また、認定個人情報保護団体はその苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることがある。

対象事業者は電気通信個人情報保護推進センターから上述の求めがあったときは、正当な理由がないのに、これを拒むことはできない。

なお、苦情処理にあたっては、電気通信事業法の消費者保護ルールに関するガイドライン(注)の第３章「苦情等の処理（事業法２７条）関係）も参照されたい。

（注）総務省ホームページで公開されている

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/syohi/pdf/090708_1.pdf

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。

２０．各種情報の取扱い

次の各種情報の取扱いにあたっては、ガイドライン第３章の規定による必要がある。なお、ガイドライン第３章に特に規定がない事項については、ガイドライン第２章の個人情報の取扱いに関する共通原則によるものとされている。

（１）通信履歴
（２）利用明細
（３）発信者情報
（４）位置情報
（５）不払い者等情報
（６）迷惑メール等送信に係る加入者情報
（７）電話番号情報

○（好ましい事例）

事例２０－１　携帯電話の利用者から、通信料金を支払わない利用者に係る不払者情報を他の携帯電話会社に提供することは個人情報の取扱いに問題があるとの苦情を受けたため、ガイドライン第２７条とその解説等を参考にして、適切な取扱いであることを説明した。

第３章　指導、勧告その他の措置（法第４３条）

【個人情報保護法】
（個人情報保護指針）
第四十三条　認定個人情報保護団体は、対象事業者の個人情報の適正な取扱いの確保のために、利用目的の特定、安全管理のための措置、本人の求めに応じる手続その他の事項に関し、この法律の規定の趣旨に沿った指針（以下「個人情報保護指針」という。）を作成し、公表するよう努めなければならない。
第2項　認定個人情報保護団体は、前項の規定により個人情報保護指針を公表したときは、対象事業者に対し、当該個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとるよう努めなければならない。

対象事業者の個人情報の取扱いが、本指針に違反していると認められるときは、当協会は、法第４３条第２項の規定に基づき、当該対象事業者に対して、次のとおり指導、勧告その他の措置をとるものとする。

１．指導

当該対象事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるよう口頭又は文書により指導するものとする。

２．勧告

前項の規定による指導を受けた対象事業者が正当な理由なくその指導に従わなかった場合において、個人の権利利益を保護するため必要があると認めるときは、当該対象事業者に対し、その指導に係る措置をとるべきことを文書により勧告するものとする。

３．その他の措置

前項の規定による勧告を受けた対象事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合には、別に定めるところにより、当該対象事業者の対象事業者たる資格を停止し、又は当該対象事業者の登録を取消すものとする。

第４章　指針の見直し

本指針は、個人情報保護に関する国民的な意識の高まり、個人情報漏えい事故の発生状況、他の事業分野において講じられている個人情報保護に係る措置の実態、情報通信技術の発展及び実務の状況等に応じて、適宜見直しをすることが必要である。そのため、本指針策定後も、随時関係者の意見を聞きながら、不断の見直しに努めていくものとする。

別紙

事　故　報　告　書

平成____年__月__日

総務省総合通信基盤局
電気通信事業部　消費者行政課　御中

会社名　　印

事故の種類	個人情報の漏えい
発生年月日	
発生場所	
発生状況	
発生原因	
措置模様	顧客対応、社内処分、再発防止策等を記入。一枚に収まりきれないときは、「別紙参照」として別紙に記載。

※　報告書の用紙の大きさは、日本工業規格Ａ列４番とすること。

参考資料１

例　１	個人情報の利用目的の一部変更のお知らせ（例）
例　２	就業時の秘密保持誓約書（例）
例　３	退職時の秘密保持誓約書（例）
例　４	個人情報保護に関する委託先との覚書（例）
例　５	プライバシーポリシー（例）
例　６	個人情報の利用目的通知申請書（例）
例　７	個人情報の利用目的の回答書（例）
例　８	個人情報の開示申請書（例）
例　９	個人情報の開示についてのお知らせ（例）
例１０	個人情報の開示及び一部非開示についてのお知らせ（例）
例１１	個人情報の非開示についてのお知らせ（例）
例１２	個人情報の訂正・追加・削除申請書（例）
例１３	個人情報の利用停止・消去申請書（例）
例１４	個人情報の第三者提供停止申請書（例）
例１５	個人情報の訂正等措置回答書（例）
例１６	委任状（例）

例１

平成〇〇年〇〇月〇〇日

個人情報の利用目的の一部変更のお知らせ（例）

個人情報の利用目的を、下記のとおり一部変更しましたので、通知・公表します。

記

１．変更点

変更前	変更後
変更する個人情報の項目（種類）とその利用目的を記載する。	左記の変更後の利用目的を記載する。

２．変更理由

３．問合わせ先

以上

例２

就業時の秘密保持誓約書（例）

例		備考
誓約書		タイトルは、誓約書、個人情報保護の誓約書、機密保持誓約書等内容を適切に表すものを付ける。
平成〇〇年〇〇月〇〇日		誓約書の記入日 採用時や秘密保持に関する社内規定変更時等、誓約書が記入された日付を記入する。
〇〇電気通信会社 〇〇〇〇　殿		会社名と誓約書の提出先（社長、人事部長、総務部長等）
氏名〇〇　〇〇		誓約書の提出者名。アルバイト等に使用する場合には住所等の連絡先の記入を求めることもある。
「私は、〇〇電気通信株式会社の従業員（※）として、次の事項を遵守し、誠実に業務を遂行することを固く誓います。」旨を誓約する。		従業員の部分は、各社において一般的に使用している「社員」、「職員」等に適宜変更する。
（1）遵守義務		
	法令及び次の（2）から（5）の義務等が規定されている社内規定を遵守すること。	少なくとも、個人情報の保護、通信の秘密の保持、これらの安全管理措置基準を定めている社内規定の遵守を規定する。
（2）報告義務		
	違法、違反行為や事故を起した場合や発見した場合などは、社内規定に従い報告すること。	具体的に誰にどのように報告するのかを誓約書に記載することが望ましい。
（3）協力義務		
	個人情報の保護、通信の秘密の保持、これらの安全管理措置のために会社が実施する施策に協力すること。	情報安全月間の活動や社内啓発活動等、具体的な施策の例が明らかな時は、これらを例示することが望ましい。

例		備考
(4)守秘義務		
	○個人情報、通信の秘密など守秘義務の対象となる事項を記載する。	守秘義務の内容は、明確に記載する必要がある。
	○それぞれの事項について、業務上知り得た情報を第三者に提供しないこと、自己又は他人のために利用しないこと、業務上の必要なく情報に触れないことなど守秘義務の内容を記載する。	
	○個人情報や通信の秘密に関する守秘義務は、就業時のみならず職を退いた後も存続することを記載する。	
(5)禁止行為		
	①情報資産の業務以外への使用の禁止(私用メールの禁止や業務と無関係なホームページへのアクセス禁止等)	情報の安全管理のために、従業者に求める禁止行為の定めがある場合には、具体的な例などをあげて分かりやすく記載することが望ましい。
	②会社が使用を認めていない情報機器等の社内持込や業務への使用の禁止	
	③会社が認めた場合以外の情報や情報機器の自宅等の社外への持出しの禁止	
	④会社の許可を得て、情報や情報機器を社外に持ち出す場合、持出しルール以外の取扱いの禁止	
	⑤その他	

例	備考
「本誓約書の各条項のいずれかに違反した場合、就業規則に定める懲戒事由に照らし罰則が適用されることがあること、これにより会社に損害を与えた場合には、その補償の責任を問われることをあらかじめ承諾します。」旨を確認する。	責任に関する記載は、明確にしておく必要がある。
以上	

例３

退職時の秘密保持誓約書（例）

例		備考
誓約書		就業時に行った秘密保持の誓約を退職時に確認するものであり、確認書等のタイトルを使用してもよい。
平成〇〇年〇〇月〇〇日		誓約書の記入日 退職時、誓約書が記入された日付を記入する。
〇〇電気通信会社 〇〇〇〇　殿		会社名と誓約書の提出先（社長、人事部長、総務部長等）
氏名〇〇　〇〇		誓約書の提出者名。アルバイト等に使用する場合には住所等の連絡先の記入を求めることもある。
「私は、貴社を退職するにあたり、次の事項について誓約します。」旨を誓約する。		
（1）通信の秘密の保護		
	在職中、貴社の取扱中に係る通信に関して知り得た他人の秘密を、退職後も守る義務があることを理解していることを確認する。	電気通信事業法等により退職後も義務付けられている通信の秘密の保護義務を確認する。
（2）個人情報の秘密保持		
	在職中、貴社の業務に関して知り得た個人情報の内容を、退職後もみだりに他人に知らせたり不当な目的に使用しない責務があることを理解していることを確認する。	ガイドラインにより退職後も求められている個人情報の秘密保持責務を確認する。また、社内規定によりその他の秘密保持が求められている場合には、その旨確認することもできる。
（3）返却の確認		
	社内規定〇〇により、個人情報が記載等された会社の書類やデータ等（コピーを含み、ハードソフトの媒体は問わない）はすべて会社に返却したことを確認する。	社内規定に、会社書類等の返却に関して定めている必要がある。

（4）無断持出し等していないことの確認		
	社内規定〇〇により、会社の許可なく社外に個人情報及び通信の秘密に係る情報を持出したり、第三者に提供していないことを確認する。	社内規定に、個人情報の外部持出し等に関して定めている必要がある。
（5）廃棄等の確認		
	社内規定〇〇により、業務上使用したすべてのデータやコピーは会社に返還したものを除き、廃棄したことを確認する。	社内規定に、個人情報の廃棄等に関して定めている必要がある。
（6）損害補償		
	本誓約書の各条項のいずれかに違反したことにより、会社に損害を与えた場合には、その補償の責任を問われることをあらかじめ承諾することを確認する。	
以上		

例４

個人情報保護に関する委託先との覚書（例）

例	備考
個人情報の取扱いに関する覚書	タイトルは、「個人情報の取扱いに関する契約書」、「個人情報保護に関する契約書」、「秘密保持に関する基本契約書」等がある
○×○×（以下「甲」という）と△△△△（以下「乙」という）は、平成__年__月__日付で締結した_____契約書に基づき甲が乙に委託した業務（以下「委託業務」という）の遂行にあたり、乙が取り扱う個人情報の保護及び管理について、次のとおり合意する。	本記載例は、別に委託に関する基本契約書があり、個人情報保護に関しては基本契約書とは別に覚書を締結するパターンとしているが、基本契約書の中で個人情報の取扱いに関する取り決めが行われている場合等もある。
第１条（目的） 本覚書は、乙が委託業務を遂行するにあたり、乙の取得個人情報の適切な取扱いを確保することを目的とする。	
第２条（定義） 「個人情報」とは生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できることとなるものを含む）をいうものとする。 ２.「取得個人情報」とは、前項に規定された個人情報のうち、乙が委託業務の遂行のために取得した次の情報のことをいうものとする。 (1)委託業務の遂行のため、乙が甲から提供を受けた個人情報 (2)委託業務の遂行のため、乙が自ら収集した個人情報 (3)委託業務の遂行にあたり、乙が業務上知り得た上記以外の個人情報	本記載例は、契約代理業者に、その保有する営業情報を主として活用する契約業務を委託する場合等を想定したものである。 委託元から提供される個人情報だけを利用する宛名印刷業務やデータ入力、編集、出力等の業務の委託の場合には、(2)委託先が自ら収集した個人情報や(3)業務上知り得た個人情報に関する定義の記載を必要としない。

第3条（取得個人情報の保護義務） 　乙は、取得個人情報の取扱いについて関係する法令、ガイドライン等を遵守するとともに、その具体的な取扱いに疑義が生じたときは、甲の指示に従うものとする。 2. 乙は、委託業務遂行にあたり、取得個人情報を機密事項としてその保護に努めるとともに、これを委託業務以外の目的に利用してはならないものとする。また、甲の事前の書面による承諾なしに、取得個人情報が記録された媒体の複写、複製及び加工してはならないものとする。 3. 乙は、取得個人情報を第三者及び業務上知る必要のない従業者（雇用関係のある従業員、派遣社員等）に開示・提供してはならないものとする。 4. 乙は、委託業務が終了し、又は解除された後においても、前3項の義務を負うものとする。 5. 本条各号に定める取得個人情報の保護義務は、委託業務に従事する従業者も、その在職中及び退職後においても同様に負うものとし、乙はこのために当該従業者に対し、必要な措置を講ずるものとする。また、乙は、甲から要求があった場合に、本項の措置を甲に明らかにしなければならない。	委託業務の内容により、所定の場所以外への媒体の持出し禁止等を記載すべき場合は、その旨の記載を行う。 　また、複写、複製を禁止する媒体の形態（書面、フロッピーディスク、コンパクトディスク、サーバ、ハードディスク等）を明確にしておく必要がある場合には、その旨の記載を行う。 　従業者に対する措置として、従業者との間の個人情報保持契約等があるが、措置内容が明確である場合には、本覚書に記載しておくことも可能である。

第４条（個人情報の収集の取扱手順） 　乙が、委託業務の遂行のために個人情報の収集を行うときは、その業務の目的を明確にし、その目的の達成のために必要な範囲内で、甲が定め、乙が承認した適法かつ公正な取扱手順に従い、個人情報を取り扱わなければならない。	委託先が、委託業務のために個人情報を収集することがない場合には、本条の規定は不要である。 　個人情報の取扱手順としては、個人情報の収集方法、本人からの同意の取得方法、保管期間、廃棄等に関するものが含まれ、取扱いの目的を明確にし、その目的達成のために必要な範囲内で、適法かつ公正な手順を定めておくことが望ましい。 　また、乙が独自の責任で収集した個人情報を甲からの委託業務に利用する場合、委託業務に利用することがその個人情報の利用目的となっているか、必要な本人の同意を乙が取得しているかなどという、乙の個人情報の取扱いに関する確認を行い、甲の委託業務に乙が収集した個人情報を利用することが適法かつ公正であることを担保するために必要な取決めを覚書等の中に盛り込むことが望ましい。
第５条（取得個人情報の取扱責任者） 　乙は、委託業務の遂行にあたり、取得個人情報の取扱責任者を定め、その指揮のもとに取得個人情報を適切に保護しなければならないものとする。 ２．乙は、取得個人情報の取扱責任者の氏名及び所属を書面により甲に通知するものとする。また、当該責任者を変更した場合も同様とする。 ３．取得個人情報の取扱責任者は、本覚書に定める事項を遵守するとともに、従業者にこれを理解・遵守させるために必要かつ適切な教育を施す責任を負うものとする。	

第6条（安全性の確保） 　乙は、善良なる管理者の注意をもって取得個人情報を管理する義務を負うものとし、取得個人情報が記録された情報処理システムに対する不正アクセス、破壊、改ざん、又は乙の取得個人情報の紛失、漏えい等の危険を防止し、取得個人情報の必要かつ適切な管理を行うための合理的な安全対策を講じるものとする。	委託先における個人情報の漏えい防止、盗用禁止、返還、消去、廃棄等の個人情報の安全管理に関する事項について記載する。
第7条（再委託の制限） 　乙は、委託業務の全部を第三者に委託してはならない。 2. 乙は、委託業務の一部を乙以外の第三者に委託することができる。この場合において、乙は、当該委託業務を遂行する能力を持つ者を、責任を持って選定することとし、事前に書面にて甲の承認を得なければならない。 3. 乙は、前項に基づき甲の承認を求める場合は、再委託の内容、再委託先、その他再委託先に対する管理方法等を書面で提出しなければならない。 4. 本条第2項の規定により乙から委託を受けた者は、本覚書により乙が履行すべき義務と同等の義務を負うものとする。乙は、その旨明記した書面を乙及び当該委託業務を受けた者との連名で甲に提出しなければならない。 5. 乙から当該委託業務を受けた者が更に他の第三者に委託してはならない。	本記載例は、委託業務の一部を委託先が他に再委託することは認めるが、再再委託することは原則認めない場合の記載例である。 　再委託をすべて禁止する場合には、「乙は、委託業務の全部又は一部を第三者に委託してはならない。」等の記載が考えられる。 　再再委託等2段階以上の委託を許す場合には、再再委託先等の選任監督に関する事項を定める必要がある。

第8条（管理状況の報告・調査） 　甲は、乙の取得個人情報の管理状況について、その必要に応じ、乙の書面による報告を求めることができるものとし、乙は速やかにこれに応じるものとする。 2. 甲は、乙の取得個人情報の管理状況を調査するため、乙に事前に通知したうえで乙の事務所等に立ち入ることができるものとし、この場合、乙は甲の調査に協力する義務を負うものとする。	委託業務の内容や委託期間により、定期的な報告や委託業務終了時の報告等を行うことが甲乙間で定まっている場合には、その旨記載する。 　また、甲による事務所立入調査のほか、報告調査の状況により、乙に対し、担当者の変更、作業手順の変更、保管・廃棄手順の変更等を求める場合があることが甲乙間で定まっている場合には、その旨を記載する。
第9条（事故発生時の措置） 　乙は取得個人情報の紛失、破壊、改ざん、漏えい等の事故が発生した場合には、ただちに甲に報告するとともに、本人からの苦情への対応等を甲と協議し、適切な措置を講じるものとする。 2. 乙は、発生した事故の再発防止策について検討し、甲と協議のうえ決定した再発防止策を乙の責任と費用負担で講じるものとする。	委託先が、委託に係る個人情報の取扱いに関する事故を起した場合、委託元と委託先の双方で事故対応を行う必要があるが、その対応は両者がよく連携して行うことが望ましい。
第 10条（損害賠償） 　前条の規定にかかわらず、乙の責に帰すべき事由により、取得個人情報の紛失、破壊、改ざん、漏えい等の事故が発生し、甲が第三者から請求を受け、又は第三者との間で紛争が発生した場合には甲及び乙は誠意をもって協議を行うとともに乙の費用負担でこれらに対処するものとする。この場合、甲が損害を被ったときは、乙は甲に対して当該損害を賠償しなければならないものとする。	事故の責任に関する規定については、委託元又は委託先のいずれかが優越的地位の濫用とならないよう両者が十分協議し、理解しておく必要がある。

第１１条（取得個人情報の返還等） 　乙は、委託業務の終了後、取得した個人情報が記録された資料等（電磁的記録を含む）を、甲の指示に従い、甲に返還するか、消去又は廃棄するものとする。ただし、甲が別に指示したときは、その指示に従うものとし、甲が希望した場合には、取得個人情報の返還、消去又は廃棄に関し甲指定の様式による証明書を発行するものとする。	特に第2条第2項（2）（委託先が独自に収集した個人情報）の取扱いについては、委託元と委託先の間で十分協議し、必要な条項を記載しておくことが望ましい。
第１２条（協議事項） 　本覚書に定めのない事項もしくは本覚書の各条項の解釈について疑義が生じた場合には、甲及び乙は誠意をもって協議し、これを解決するものとする。	訴訟等の場合の管轄裁判所を定めておく場合もある。
上記覚書締結の証として本覚書2通を作成し、甲乙記名捺印のうえ、各１通を保有する。 平成____年____月____日 （甲） （乙）	

例５

プライバシーポリシー（例）

（注）プライバシーポリシーの具体的な作成にあたっては、「１１．プライバシーポリシー」にある記載例や好ましい事例も参照されたい。

例	備考
制定：0000 年 00 月 00 日 改正：0000 年 00 月 00 日	制定日及び改正の履歴を明らかにすることが望ましい。
プライバシーポリシー	電気通信事業者の個人情報の取扱いに関する方針についての宣誓を示すものであり、「プライバシーポリシー」、「個人情報保護指針」、「個人情報の取扱いに関する基本方針」等この主旨を表す名称を各事業者において定める。
○○○○株式会社 代表取締役社長　○○　○○	代表者が責任を有していることを明らかにすることが望ましい。
当社は、個人情報の取扱いに関する方針を、次のとおり定め、これを公表するとともに遵守することを宣言します。	ガイドライン第１４条に規定するプライバシーポリシーの記載例である。
（法令等の遵守） １．当社は、お客様の個人情報の取得、利用その他一切の個人情報の取扱いについて、個人情報の保護に関する法律、通信の秘密に係る電気通信事業法の規定その他の関連法令、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（以下、「ガイドライン」といいます）、及びこのプライバシーポリシーを遵守します。	ガイドライン第3条の一般原則を遵守することを定める。

（利用者の権利利益の保護に関する取組） 2．当社は、個人情報保護に関する利用者の権利利益の保護のための主な取組として次を実施しています。 ① 本人の求めがあった場合、ダイレクト・メールの発送停止や電話勧奨の停止措置等を行います。（詳しくは〇〇にお問い合わせ下さい。） ② 当社は個人情報の取扱いの全部又は一部を利用目的の範囲内で委託します。 委託先は、個人情報を適正に取り扱うと認められるものを選定し、委託契約において、安全管理、秘密保持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、必要かつ適切な監督を行います。 なお、委託する主な事務は次のとおりです。 ◎各種商品・サービスの販売・受付業務 ◎故障修理業務 ◎料金関連業務 ◎マーケティング業務 ③ ※※※に示すように、利用者ごとに利用目的を限定しています。 ④ 個人情報の取得方法等については、△△にてご案内致します。	利用者の権利利益の保護に関する具体的な取組を可能な限り記載することが望ましいが、この項の内容については、「ダイレクト・メール等の停止措置」、「個人情報の委託」、「利用目的の特定」、「適正な取得」等として別途記載しても差し支えない。 ① 〇〇には電話番号やリンク先を記載する。 ② 委託先等に関する問合わせに応じる場合には、その連絡先を記載する。 ③ ※※※は、ガイドライン第8条第1項に基づき、利用目的を公表しているところを示している。 ④ 「5．適正な取得」において、取得元や取得方法（取得源の種類等）を明らかにする旨を記載している場合には「5．適正な取得を参照して下さい。」との記載でもよい。
（利用目的の特定及び公表） 3．当社は、当社が取得したお客様の個人情報の利用目的をできる限り特定の上、あらかじめ公表します。また、お客様から契約書等の書面に記載された個人情報を直接取得する場合は、あらかじめお客様に対して利用目的を明示します。利用目的については、※※※をご覧下さい。	ガイドライン第5条は「利用目的をできる限り特定する」としているが、各電気通信事業者の判断により「利用目的を特定する」と宣言することも可能である。 ※※※は、ガイドライン第8条第1項に基づき、利用目的を公表しているところを示している。 他の企業等から個人情報の取扱いを受託する場合には、当該個人情報に関する利用目的も公表等することが求められている。

（利用目的の範囲内での利用） 4．当社は、あらかじめ特定し公表した利用目的の達成に必要な範囲内でのみお客様の個人情報を取り扱います。ただし、次の各号に該当する場合は、お客様の同意を得ることなく、あらかじめ特定し公表した利用目的の達成に必要な範囲を超えてお客様の個人情報（通信の秘密に係る情報は除く。）を取り扱うことがあります。 1）法令に基づく場合 2）人の生命、身体又は財産の保護のために必要がある場合であって、お客様本人の同意を得ることが困難であるとき 3）公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、お客様本人の同意を得ることが困難であるとき 4）国の機関若しくは地方公共団体又はその委託を受けた者が法令に定める事務をすることに対して協力する必要がある場合であって、お客様本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき	1）～4）の記載に替えて、「ガイドライン第6条第3項の各号に該当する場合」と記載しても差支えない。 ただし書き以下は、第三者提供の例外事項と重複する内容でもあり、この項ではあえて記載しなくても差し支えない。
（適正な取得） 5．当社は、偽りその他不正の手段により個人情報を取得しません。 また、個人情報の取得方法等については、△△にてご案内致します。	少なくともガイドライン第 7 条の「適正な取得」を宣言しておくことが望ましい。また、取得元や取得方法（取得源の種類等）を明らかにする場合には、その旨を記載することが望ましい。
（保存期間） 6．当社は、利用目的に必要な範囲内でお客様の個人情報の保存期間を定め、保存期間経過後又は利用目的達成後はお客様の個人情報を遅滞なく消去いたします。ただし、次の各号に該当する場合はこの限りではありません。 1）法令の規定に基づき、保存しなければならないとき。 2）本人の同意があるとき。	1）～2）の記載に替えて、「ガイドライン第10条第2項の各号に該当する場合」と記載しても差支えない。

（安全管理措置） 7. 当社は、お客様の個人情報を正確かつ最新の内容に保つよう努めるとともに、不正なアクセス、改ざん、漏えい、滅失及び毀損から保護するため、必要かつ適切な安全管理措置を講じます。	ガイドライン第１１条の安全管理措置を講ずることを定める。
（従業者の監督） 8. 当社は、お客様の個人情報の安全管理が図られるよう従業者に対する必要かつ適切な監督をします。また、従業者に対して個人情報の適正な取扱いの確保のために必要な教育研修を実施します。	ガイドライン第１２条第１項及び第２項の規定に基づき従業者の監督を行うことを定める。
（委託先の監督） 9. 当社は、各種商品・サービスの販売・受付業務、故障修理業務、料金関連業務、マーケティング業務その他の業務において、個人情報の取扱いの全部又は一部を利用目的の範囲内で委託します。この場合において、当社は、個人情報を適正に取り扱うと認められるものを選定し、委託契約において、安全管理、秘密保持、再委託の条件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、必要かつ適切な監督を実施します。	ガイドライン第１２条第３項及び第４項の規定に基づく、委託先の監督を行うことを定める。 委託する業務の内容は、各電気通信事業者の業務実態に即して記載する。
（第三者への提供） 10. 当社は、次の各号に掲げる場合を除き、お客様の同意を得ないで、第三者にお客様の個人情報を提供することはしません。 1）法令に基づく場合 2）人の生命、身体又は財産の保護のために必要がある場合であって、お客様本人の同意を得ることが困難であるとき 3）公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、お客様本人の同意を得ることが困難であるとき 4）国の機関若しくは地方公共団体又はその委託を受けた者が法令に定める事務をすることに対して協力する必要がある場合であって、お客様本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき	1）～4）の記載に替えて、「ガイドライン第１５条第１項の各号に該当する場合」と記載しても差支えない。

（開示等の求め） 11．お客様が個人情報の利用目的の通知、又は個人情報の開示、又は訂正、追加若しくは削除又は利用の停止若しくは第三者への提供の停止を希望される場合は、当社が別に定める手続に従って下さい。個人情報の開示等の求めの手続は、＃＃＃をご覧下さい。	＃＃＃は、ガイドライン第16条に基づき個人情報に関する事項の公表しているところを示している。
（苦情の処理） 12．当社は、個人情報の取扱いに関するお客様からの苦情その他のお問い合わせについて迅速かつ適切に対応いたします。苦情その他のお問い合わせは以下にて承っております。 （対応窓口の名称） （対応窓口の連絡先） （対応窓口の受付時間）	ガイドライン第21条に基づき苦情処理するための苦情受付窓口を定める。
（認定個人情報保護団体） 13．当社は、認定個人情報保護団体である財団法人日本データ通信協会の対象事業者です。当社の個人情報の取扱いに関する苦情については、財団法人日本データ通信協会内に設けられている電気通信個人情報保護推進センターへ解決の申出をすることもできます。 「電気通信個人情報保護推進センター」 電話：03－5907－3803 （平日10時～12時、13時～17時） E－mail： privacy@dekyo.or.jp	ガイドライン第21条に基づき苦情処理するため、認定個人情報保護団体財団法人日本データ通信協会の対象事業者となった場合、電気通信個人情報保護推進センターを案内する。
（漏えい発生時の対応） 14．お客様の個人情報の漏えい等が発生した場合には、事実関係を速やかにお客様に通知するなど適切な対応を行います。	ガイドライン第22条に基づき適切な措置をとることを宣言することが望ましい。
（継続的改善） 15．当社は、個人情報保護に関する内部規定の整備、従業者教育及び内部監査の実施などを通じて、社内における個人情報の取扱いについて継続的な改善に努めます。	継続的改善を定めることは重要である。

例６

個人情報の利用目的通知申請書（例）

平成〇〇年〇〇月〇〇日

〇〇株式会社（個人情報取扱窓口）御中

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 24 条第 2 項及び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）第 16 条第 2 項の規定に基づき、〇〇株式会社の保有する個人情報につき、下記のとおり、その利用目的の通知を求めます。

記

◎申請対象となる本人を特定するための事項

本人を特定する事項	本人の氏名、住所等（必要最小限の情報に限定する必要がある。）

◎申請者を確認するための事項

本人が申請する場合	本人確認書類を列記
法定代理人が申請する場合	法定代理人の種類を記載し、その資格を証明する書類及び法定代理人自身の確認書類を列記
任意代理人が申請する場合	本人からの委任状、本人に関する確認書類及び代理人自身の確認書類を列記

◎申請対象となる個人情報を特定する事項

申請対象を特定するために必要な情報	サービスに関係して保有している個人情報（お名前、住所、電話番号、メールアドレス等）を列挙し、本人の特定を容易にすることが望ましい。
	契約以外の場合において、アンケート、イベント、懸賞、モニター募集等個人情報を取得した機会を記載する欄を設けることなど、本人の特定を容易にすることが望ましい。
	通知を求める利用目的の時期（平成　　年　　月　　日において公表されていた利用目的等）

◎手数料

（手数料を設定している場合は、手数料額とその納付方法を記載する。）

◎受付方法

（この利用目的通知申請の受付方法及びその窓口に関する情報を記載する。）

注意事項（例）

- 最新の個人情報の利用目的は、〇〇において公表しており、××で無料で問合わせに応えていること。
- 手数料が全額支払われるまで、申請はないものとして扱うこと。
- 法第 18 条第 4 項各号に該当する場合や、申請の対象が特定されていない場合又は特定が不完全な場合には、申請に応じられないこと。
- 一部又は全部の申請に応じられない場合にも手数料は返還されないこと。
- 本申請書への回答は「本人限定受取郵便」により行うこと。
- 本申請書にて提供を受けた個人情報の利用目的や保存期間等。
- その他。

以上

例７

個人情報の利用目的の回答書（例）

平成〇〇年〇〇月〇〇日

申請者の氏名　様

電気通信事業者住所
電気通信事業者名
連絡先

平成　　年　　月　　日付貴信により、通知の求めのあった「個人情報の利用目的」について、下記のとおり、回答します。

記

◎　利用目的通知の求めの対象となっている個人情報

個人情報に係る本人	本人の氏名、住所（開示の求めに記載された内容）
個人情報の項目	通知の求めで特定された事項

◎回答内容

□	申請に係る個人情報の利用目的は、次のとおりです。 （又は、添付のとおりです。）
□	申請に係る個人情報の利用目的が特定されていないため、回答できかねます。
□	申請に係る個人情報の利用目的は、次のとおり明らかになっています。 （公表されているプライバシーポリシーのURLや契約約款の箇所等を示す。）
□	申請に係る個人情報の利用目的を通知することは、次に該当するため、通知できません。 □　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるため。 □　利用目的を本人に通知し、又は公表することにより当社の権利又は正当な利益を害するおそれがあるため。 □　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるため。

以上

例８

個人情報の開示申請書（例）

平成〇〇年〇〇月〇〇日

〇〇株式会社（個人情報取扱窓口）御中

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 25 条及び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）第 17 条第 1 項の規定に基づき、貴社が保有する下記記載の本人の「個人情報」の開示を求めます。

記

◎申請対象となる本人を特定するための事項

本人を特定する事項	本人の氏名、住所等（必要最小限の情報に限定する必要がある。）

◎申請者を確認するための事項

本人が申請する場合	本人確認書類を列記
法定代理人が申請する場合	法定代理人の種類を記載し、その資格を証明する書類及び法定代理人自身の確認書類を列記
任意代理人が申請する場合	本人からの委任状、本人に関する確認書類及び代理人自身の確認書類を列記

◎申請対象となる個人情報を特定する事項

申請対象を特定するために必要な情報	保有している個人情報の項目（名前、住所、電話番号、メールアドレス等）を列挙し、本人の特定を容易にすることが望ましい。

◎手数料

（手数料を設定している場合は、手数料額とその納付方法を記載する。）

◎受付方法

（この開示申請の受付方法及びその窓口に関する情報を記載する。）

注意事項（例）

- 手数料が全額支払われるまで、申請はないものとして扱うこと。
- 通信の秘密に属する事項等法第25条に該当する場合には、開示申請に応じられないことがあること。
- 本人確認書類の不備や、申請対象となる個人情報の特定がされていない場合や不完全な場合には、開示申請に応じられないことがあること。
- 一部又は全部の申請に応じられない場合にも手数料は返還されないこと。
- 本申請書への回答は「本人限定受取郵便」により行うこと
- 本申請書にて提供を受けた個人情報の利用目的や保存期間等
- 通話明細を希望される場合には、〇〇にて申出を受けていること。
- その他

以上

例９

個人情報の開示についてのお知らせ（例）

平成〇〇年〇〇月〇〇日

申請者の氏名　様

電気通信事業者住所
電気通信事業者名
連絡先

個人情報の開示についてのお知らせ（例）

平成　　年　　月　　日付貴信により、開示の求めのあった「個人情報」について、下記のとおり、ご連絡します。

記

◎　申請対象の個人情報

個人情報に係る本人	本人の氏名、住所（開示の求めに記載された内容）
個人情報の項目	（開示の求めで特定された事項）

◎　開示する個人情報

（開示する個人情報の内容を記載する。）
（「添付のとおり開示します。」として、開示対象の個人情報を添付してもよい。）

以上

例１０

個人情報の開示及び一部非開示についてのお知らせ（例）

平成〇〇年〇〇月〇〇日

申請者の氏名　様

電気通信事業者住所
電気通信事業者名
連絡先

平成　　年　　月　　日付貴信により、開示の求めのあった「個人情報」について、一部開示しないこととしましたので、開示する個人情報及び開示しない個人情報とその理由を、下記のとおりご連絡します。

記

◎　申請対象の個人情報

個人情報に係る本人	本人の氏名、住所（開示の求めに記載された内容）

◎開示する個人情報

個人情報の項目	開示の求めで特定された事項
（開示する個人情報の内容を記載する。） （「添付のとおり開示します。」として、開示対象の個人情報を添付してもよい。）	

◎非開示とした個人情報とその理由

（非開示とした個人情報）

個人情報の項目	開示の求めで特定された事項

（非開示とした理由）

□　申請対象の個人情報が特定されていません。 □　開示の求めに係る個人情報を保有していません。 □　次の理由により開示しないこととしました。 □本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるため。 □当社の業務の適正な実施に著しい支障を及ぼすおそれがあるため。 □他の法令に違反することとなるため。（法令名：　　）

以上

例１１

個人情報の非開示についてのお知らせ（例）

平成〇〇年〇〇月〇〇日

申請者の氏名　様

電気通信事業者住所
電気通信事業者名
連絡先

平成　　年　　月　　日付貴信により、開示の求めのあった「個人情報」について、開示しないこととしましたので、下記のとおりご連絡します。

記

◎　申請対象の個人情報

個人情報に係る本人	本人の氏名、住所（開示の求めに記載された内容）
個人情報の項目	（開示の求めで特定された事項）

◎　開示しないこととした理由

□　本人確認ができませんでした。
　□申請書に記載されている情報と本人確認のための書類に記載されている情報が一致していません。（不一致情報：　　）
　□代理人による申請に際して、代理権の確認が不可能です。
□　申請書類に不備がありました。（不備申請書類：　　）
　（不備内容：　　）
□　申請対象の個人情報が特定されていません。
□　開示の求めに係る個人情報を保有していません。
□　次の理由により開示しないこととしました。
　□本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるため。
　□当社の業務の適正な実施に著しい支障を及ぼすおそれがあるため。
　□他の法令に違反することとなるため。（法令名：　　）

以上

例１２

個人情報の訂正・追加・削除申請書（例）

平成〇〇年〇〇月〇〇日

〇〇株式会社（個人情報取扱窓口）御中

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 26 条第 1 項及び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）第 17 条第 3 項に基づき、貴社が保有する下記記載の本人の「個人情報」の内容の訂正、追加又は削除を求めます。

記

◎申請対象となる本人を特定するための事項

本人を特定する事項	本人の氏名、住所等（必要最小限の情報に限定する必要がある。）

◎申請者を確認するための事項

本人が申請する場合	本人確認書類を列記
法定代理人が申請する場合	法定代理人の種類を記載し、その資格を証明する書類及び法定代理人自身の確認書類を列記
任意代理人が申請する場合	本人からの委任状、本人に関する確認書類及び代理人自身の確認書類を列記

◎申請対象となる個人情報を特定する事項

申請対象を特定するために必要な情報	個人情報（名前、住所、電話番号、メールアドレス等）を列挙し、本人の特定を容易にすることが望ましい。

◎申請する措置とその理由

	訂正	訂正する内容	理由（事実でない、保存期間が経過している、当該個人情報の取扱いが適正でない等の理由を列記）
	追加	追加する内容	
	削除	削除する内容	

◎受付方法

（この訂正等申請の受付方法及びその窓口に関する情報を記載する。）

注意事項（例）

- 契約者の氏名、住所、連絡先等の変更の場合には、〇〇にて申出を受けていること。
- 訂正等の申請に理由がない場合には、これに応じられないことがあること。
- 本人確認書類の不備や、申請対象となる個人情報の特定がされていない場合や不完全な場合には、訂正等の申請に応じられないことがあること。
- 本申請に対する措置に関する回答方法
- 本申請書にて提供を受けた個人情報の利用目的や保存期間等
- その他

以上

例１３

個人情報の利用停止・消去申請書（例）

平成〇〇年〇〇月〇〇日

〇〇株式会社（個人情報取扱窓口）御中

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 27 条第 1 項及び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）第 17 条第 3 項の規定に基づき、貴社が保有する下記記載の本人の「個人情報」の利用の停止（又は消去）を求めます。

記

◎申請対象となる本人を特定するための事項

本人を特定する事項	本人の氏名、住所等（必要最小限の情報に限定する必要がある。）

◎申請者を確認するための事項

本人が申請する場合	本人確認書類を列記
法定代理人が申請する場合	法定代理人の種類を記載し、その資格を証明する書類及び法定代理人自身の確認書類を列記
任意代理人が申請する場合	本人からの委任状、本人に関する確認書類及び代理人自身の確認書類を列記

◎申請対象となる個人情報を特定する事項

申請対象を特定するために必要な情報	個人情報（名前、住所、電話番号、メールアドレス等）を列挙し、本人の特定を容易にすることが望ましい。

◎申請する措置とその理由

	利用停止	理由（目的外利用、不正な取得、保存期間を経過している等の理由を列記）
	消去	

◎受付方法

（この利用停止等申請の受付方法及びその窓口に関する情報を記載する。）

注意事項（例）

- サービス勧奨等のための DM 送付、電子メール送信、電話勧誘等のための利用停止の依頼の場合、〇〇にて申出を受けていること。
- 利用停止等の申請に理由がない場合には、これに応じられないことがあること。
- 本人確認書類の不備や、申請対象となる個人情報の特定がされていない場合や不完全な場合には、利用停止等の申請に応じられないことがあること。
- 本申請に対する措置に関する回答方法
- 本申請書にて提供を受けた個人情報の利用目的や保存期間等
- その他

以上

例１４

個人情報の第三者提供停止申請書（例）

平成〇〇年〇〇月〇〇日

〇〇株式会社（個人情報取扱窓口）御中

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 27 条第 2 項及び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）第 17 条第 3 項の規定に基づき、貴社が保有する下記記載の本人の「個人情報」の第三者への提供の停止を求めます。

記

申請対象となる本人を特定するための事項

本人を特定する事項	本人の氏名、住所等（必要最小限の情報に限定する必要がある。）

申請者を確認するための事項

本人が申請する場合	本人確認書類を列記
法定代理人が申請する場合	法定代理人の種類を記載し、その資格を証明する書類及び法定代理人自身の確認書類を列記
任意代理人が申請する場合	本人からの委任状、本人に関する確認書類及び代理人自身の確認書類を列記

申請対象となる個人情報を特定する事項

申請対象を特定するために必要な情報	個人情報（名前、住所、電話番号、メールアドレス等）を列挙し、本人の特定を容易にすることが望ましい。

申請する措置とその理由

措置（誰に対する第三者提供を停止するか等求める措置を記載） 理由（同意していない等の理由を記載）

◎受付方法

（この第三者提供停止申請の受付方法及びその窓口に関する情報を記載する。）

注意事項（例）

- 第三者提供停止の申請に理由がない場合には、これに応じられないことがあること。
- 本人確認書類の不備や、申請対象となる個人情報の特定がされていない場合や不完全な場合には、第三者提供停止申請に応じられないことがあること。
- 本申請に対する措置に関する回答方法
- 本申請書にて提供を受けた個人情報の利用目的や保存期間等
- その他

以上

例１５

個人情報の訂正等措置回答書（例）

平成〇〇年〇〇月〇〇日

申請者の氏名　様

電気通信事業者住所
電気通信事業者名
連絡先

平成　　年　　月　　日付貴信により、訂正等の求めのあった「個人情報」について、措置の結果を、下記のとおり回答します。

記

◎　申請対象の個人情報

個人情報に係る本人	本人の氏名、住所（訂正等の求めに記載された内容）
個人情報の項目	（訂正等の求めで特定された事項）

◎申請された措置

□訂正	□追加	□削除	□利用停止	□消去	□第三者提供の停止

◎当社が行った措置

◎申請された措置の全部又は一部についてその措置を取らない場合又はその措置とは異なる措置をとる場合の理由

□本人確認ができませんでした。
□申請書に記載されている情報と本人確認のための書類に記載されている情報が一致していません。（不一致情報：　　）
□代理人による申請に際して、代理権の確認が不可能です。
□申請書類に不備がありました。（不備申請書類：　　）
（不備内容：　　）
□申請対象の個人情報が特定されていません。
□当社は訂正等の求めに係る個人情報を保有していません。
□調査の結果、個人情報の保護に関する法律（平成15年法律第57号）及び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）に違反した取扱いを行っているとは認められませんでした。
□当社が講じた措置により、個人情報の保護に関する法律（平成15年法律第57号）及び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）に違反した取扱いは是正されます。
□保存期間が経過しておらず、利用目的も達成されていません。
□求めに理由がありません。（理由不備内容：　　）

以　上

例１６

委　　任　　状（例）

平成〇〇年〇〇月〇〇日

（あて先）

〇〇電気通信株式会社

代理人

ﾌﾘｶﾞﾅ	
氏名	
住所	〒　　－

私は、上記の者を代理人と定め、下記の案件及びこれに関する貴社との交渉行為に関する事項を委任します。

（委任する事項を次の項目から選ぶか、具体的に記入して下さい。）

	個人情報の開示の求め
	個人情報の訂正の求め
	個人情報の追加の求め
	個人情報の削除の求め
	個人情報の利用の停止の求め
	個人情報の第三者提供の停止の求め
	個人情報の利用目的の通知の求め
	その他（具体的に記入して下さい。）

ご本人

ﾌﾘｶﾞﾅ	
氏名	印
住所	〒　　－

参考資料２

ノートブック型パーソナルコンピュータ等の社外への持出しにおける適切な技術的保護措置について

平成22年11月17日
財団法人日本データ通信協会
電気通信個人情報保護推進センター

1．はじめに

電気通信個人情報保護推進センターでは、「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（以下「ガイドライン」という。）」において新たに規定された「個人情報漏えい等の発生時における手続（本人への通知、公表、総務省への報告）を簡略化することが可能な適切な技術的保護措置」の内容について、ガイドラインが適用される電気通信事業者に対して、できるだけ具体的な説明等を示すことにより、ノートブック型パーソナルコンピュータ等による情報資産の社外への持出しに伴うリスクに対応した適切な技術的保護措置の導入を促すことを目的として、本解説を作成した。

適切な技術的保護措置の対象は、ガイドライン第22条の規定に基づき「ノートブック型パーソナルコンピュータ等」が対象となる。「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メモリ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が想定されている。

なお、個人情報の漏えい等の発生時における手続（本人への通知、公表、総務省への報告）を簡略化することが可能な「適切な技術的保護措置」が講じられている場合とは、Ⅰ高度な暗号化措置が講じられていること、Ⅱ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、Ⅲ個人情報漏えい等に際し、Ⅰ及びⅡ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が、これらのⅠ、Ⅱの条件に該当する例、該当しない例を次の表に例示するので参考にされたい。

（注）本解説は、平成22年11月時点における技術的な背景に基づいて適切な技術的保護措置についてまとめたものであるが、時間を経るごとに技術の安全性が変化することや、より安全な技術が登場することも考えられるため、適切な技術的保護措置については、必要に応じて見直しを実施する。

Ⅰ　高度な暗号化措置が講じられていること。

＜○　Ⅰに該当する例＞

ⅰ　暗号化機能付き記録媒体（①）

専用の暗号化チップにより、媒体上に書かれるデータがすべて自動的に暗号化、復号化されるため、個人情報の保存先として利用可能な領域のすべてが暗号化される。（ハードディスク、SSD（Solid State Drive：フラッシュメモリを利用した記録媒体）等において製品が販売されている。）

ⅱ　ディスク暗号化ソフトウェア（②）

暗号化専用のソフトウェア（FDE SoftWare：Full Disk Encryption SoftWare）により、OSやプログラム、データがすべて自動的に暗号化、復号化される。暗号化ソフトウェアが格納された領域等、一部の領域は暗号化されないが、これらは個人情報の保存先として利用不可能な領域であるため問題はない。

＜×　Ⅰに該当しない例＞

ⅰ　特定ファイルのみを指定した暗号化

OSが起動後、OS上のアプリケーションとして暗号化ソフトウェアが起動する場合で、暗号化したいファイルやフォルダを指定したうえで、その対象のみが暗号化される。暗号化処理を行ったファイルやフォルダ以外、通常のOS領域、データ領域が暗号化されておらず、一時データが暗号化されずに残っている可能性があるため、対象とならない。

Ⅱ　適切な暗号化された情報及び復号鍵の管理がされていること。

Ⅱ－1　復号鍵のすべてが暗号化された情報と分離されている。

＜○　Ⅱ－1に該当する例＞

ⅰ　パソコンを紛失したが、パソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っている場合。また、予備のUSBメモリがある場合は、その存在も確認できることが必要である。（③）

＜×　Ⅱ－1に該当しない例＞

ⅰ　パソコンとパソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリを同時に紛失した場合。また、USBメモリが手元に残っている場合でも、予備のUSBメモリが存在し、その存在が確認できない場合。

ⅱ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリは手元に残っているが、そのUSBメモリ内の鍵が容易に複製できた状態（例えば単純なファイルコピーや記憶領域全体の複製による）であり、複製が行われていないことを確認できない場合。

ⅲ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っているが、紛失したパソコンにおいて鍵とは異なる手段（例えば回避パスワードの入力）による復号化や、特定のキーワード入力による鍵の再生成が可能な場合。

Ⅱ－2　秘密分散技術によって復号鍵が分散保存されている。

＜○　Ⅱ－2に該当する例＞

ⅰ　原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、当該パソコンに格納した分散された鍵データだけでは当該パソコンの暗号化された個人情報を復号できない場合であって、分散された鍵データの一部を格納したUSBメモリ等が手元に残っている場合。（④）

ⅱ　原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、分散された鍵データの一部を権利者が管理するサーバ等に格納している場合等、紛失していない分散された鍵データが権利者の管理下にある場合。（⑤）

	＜× Ⅱ－2に該当しない例＞ ⅰ 原理的に部分復号の可能性がある方式による秘密分散技術を用いた場合。例えば鍵を分散保持した場合に、分散保持された一部のデータより鍵の全体もしくは一部が推定される可能性のある方式を用いて鍵の分散管理を行ったパソコンを紛失した場合。 ⅱ 鍵の復元に必要な数の分散鍵データが権限者の管理下に無い場合。あるいは鍵の復元に必要な数の分散鍵データが紛失した場合。

（注）上の表に示された例示について、適切な技術的保護措置が講じられているとされる具体的な組合せは、電子政府推奨暗号リスト又はISO/IEC 18033 に掲げられている暗号アルゴリズムを使用していることを前提に、次の6つの場合が該当する。

①と③が共に満たされ有効に実施されている場合

①と④が共に満たされ有効に実施されている場合

①と⑤が共に満たされ有効に実施されている場合

②と③が共に満たされ有効に実施されている場合

②と④が共に満たされ有効に実施されている場合

②と⑤が共に満たされ有効に実施されている場合

2. 適切な安全管理措置について

（1）概要

個人情報漏えい等の発生時における手続を簡略化することが可能な「適切な技術的保護措置」が講じられている場合とは次のとおりである。

なお、本解説で引用したガイドライン第22条及び解説に付記した項目番号や語句等については、説明の都合上、ガイドライン及び解説に使用されているものとは異なるものがあるので注意を要する。

Ⅰ　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/IEC 18033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。

Ⅱ　適切な暗号化された情報及び復号鍵の管理がされていること。

次の（ア）又は（イ）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可能な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、（ア）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、（イ）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。

（ア）次のA又はB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。

A　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。

B　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。

（イ）遠隔操作により記録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、記録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。

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

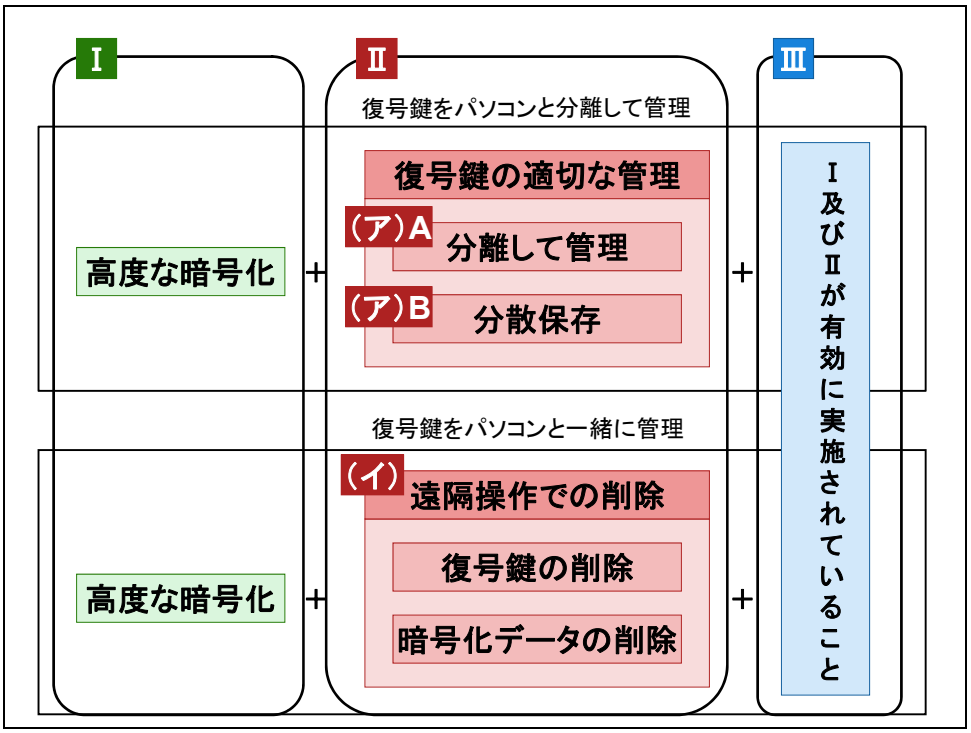


図１ 適切な安全管理措置の概要

対象となる個人情報が高度な暗号アルゴリズム（暗号化の処理手順）により暗号化されていれば、一般には第三者がその個人情報を取得しても、それを解読すること等は困難である（Ⅰ）。ただし、高度な暗号化が施されていたものの、個人認証であるパスワード等や鍵の管理が不十分な場合には暗号化措置を施していた意味がなくなるため、鍵を適切に管理することが重要となる（Ⅱ）。また、個人情報の漏えい時にⅠ及びⅡが実際に機能していることが必要であることから、Ⅲを要件としている。（Ⅰ～Ⅲの詳細については、次の「（2）個別条項の解説」を参照。）

なお、個人認証については、パスワード等の記憶による認証、ICカード等の所有物による認証、指紋等の生体情報による認証等、様々な技術が存在するが、現状ではセキュリティー強度の評価基準が未定であること、また紛失時において、個人認証が機能していたかを確認するための有効な確認手段がないと考えられることから、今回のガイドライン改正では適切な技術的保護措置の要件として具体化せず、将来のガイドライン見直し時に再検討されることになっている。

時間を経るごとに技術の安全性が変化することや、より安全性の高い技術が登場することも考えられるため、適切な技術的保護措置については、総務省において、必要に応じて見直しが行われる。

（2）個別条項の解説

Ⅰ　高度な暗号化措置が講じられていること。
　①電子政府推奨暗号リスト又はISO/IEC 18033 に掲げられている暗号アルゴリズムによって、②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③自動的に暗号化されること。

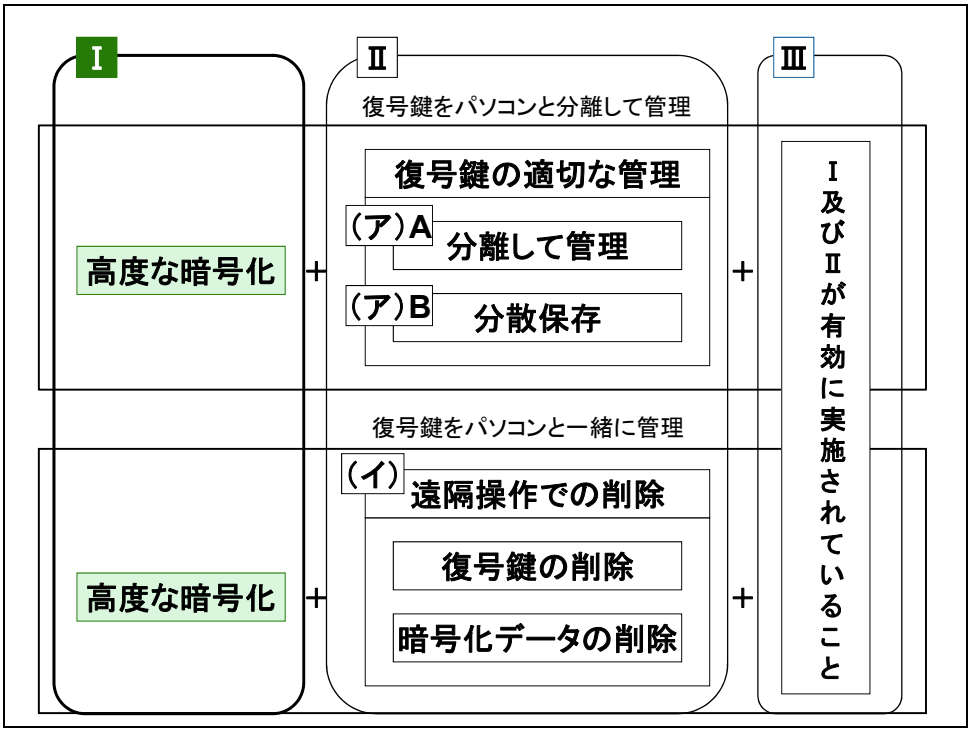


図 2 適切な安全管理措置の概要（Ⅰ　高度な暗号化措置）

（解説）

対象となる個人情報が高度な暗号アルゴリズムにより暗号化されていれば、一般には第三者がその個人情報を取得しても、それを解読すること等は困難である。

①「電子政府推奨暗号リスト又はISO/IEC 18033に掲げられている暗号アルゴリズム」とは次の表1に示すものを指す。暗号化アルゴリズムには、主に本人確認に利用する公開鍵暗号、主にデータの暗号化に利用する共通鍵暗号、主に改竄検知に用いるハッシュ関数があり、ここではハードディスクに格納されている大きなサイズの情報を暗号化することが前提であるため、実質的には共通鍵暗号が対象となると考えられる（可能であれば、公開鍵暗号、ハッシュ関数でも対象となる）。

なお、表中にあるそれぞれのアルゴリズムには、期限や条件が付されているもの等もあ

るため、実際に利活用する場合には、原典を確認することが必要である。

	電子政府推奨暗号 （平成15年度版）（注1、2） 公表元：総務省、経済産業省 原案策定：CRYPTREC（注3）	ISO/IEC 18033シリーズ（注4） 国際標準規格 策定：ISO/IEC JTC 1/SC27（注5）
公開鍵暗号		
署名	RSA-PSS(1024bit)、 RSASSA-PKCS1-V1_5(1024bit) DSA(1024bit)、ECDSA(160bit)	記載なし（ISO/IEC 9796-2等で規定）
守秘	RSA-OAEP(1024bit)、 RSAES-PKCS1-V1_5(1024bit)	RSA-KEM、RSA-OAEP、 PSEC-KEM、ACE-KEM、 HIME(R) 、ECIES-KEM
鍵共有	PSEC-KEM（160bit）、 DH(1024bit)、ECDH(160bit)	記載なし（ISO/IEC11770-3 で規定）
共通鍵暗号		
64 bitブロック暗号	3-key TDES、MISTY1、 Hierocrypt-L1、 CIPHERUNICORN-E	TDES(3-key推奨)、 MISTY1、CAST-128
128 bitブロック暗号	AES、 Camellia、SC2000、 CIPHERUNICRON-A、 Hierocrypt-3	AES、Camellia、SEED
ストリーム暗号	MUGI、MULTI-S01、 RC4(128bit)	MUGI、MULTI-S01、 SNOW 2.0
ハッシュ関数		
	SHA-256、SHA-384、SHA-512、 SHA-1、RIPEMD-160	記載なし（ISO/IEC 10118 で規定）

表１ 電子政府推奨暗号リスト又は ISO/IEC 18033 に掲げられている暗号アルゴリズム

（注1）総務省及び経済産業省が共同で開催する暗号技術検討会等において、暗号を公募の上、客観的に評価し、平成15年2月20日に、「電子政府」における調達のための推奨すべき暗号（電子政府推奨暗号）のリスト（電子政府推奨暗号リスト）を決定、公表したもの。

（注2）平成25年度から新たな推奨暗号の体系に移行することから、現在、リスト見直しのための検討が行われている。なお、160ビットハッシュ関数のSHA-1については、新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256

ビット以上のハッシュ関数を選択することが望ましいとされている。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。なお、既に危殆化が認められる暗号アルゴリズムについては採用しない、又は他の危殆化の無いアルゴリズムへ速やかな変更を行うことが望ましい。

（注3）CRYPTREC : Cryptography Research and Evaluation Committees事務局（総務省、経済産業省、NICT、IPA）

（注4）情報セキュリティーに関する国際標準化を行うISO/IEC JTC1 SC27(IT Security Techniques/セキュリティー技術)により策定され発行された、暗号に関する国際標準規格。ISO/IEC 18033は4つのパートから構成されるマルチパートの規格であり、パート1は総論、パート2に非対象暗号、パート3にブロック暗号、パート4にストリーム暗号がそれぞれ規定されている。

（注5）ISO / IEC Joint Technical Committee 1 / SubCommittee 27 “IT Security techniques”
ISO: International Organization for Standardization （国際標準化機構）
IEC: International Electrotechnical Commission （国際電気標準会議）

② 「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」とは、ハードディスクのうち、OSが管理する部分と利用者が管理する部分の両方をいう。（記録媒体とはパソコンのハードディスク、CD－ROM、USBメモリ等を指すが、ここではパソコンのハードディスクを対象とする。）

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としては、ハードディスクのフルボリューム（ハードディスクは「ボリューム」と呼ばれる管理単位で構成され、「フルボリューム」とはすべてのボリューム、すなわちハードディスクの全領域のことを指す。）が想定されるが、例えばパソコンの仕様上、個人情報が記録されることがまったく無い領域、例えば、ハードディスクの製造メーカにのみ利用される領域等は暗号化の対象外としている。

なお、ガイドラインの対象は個人情報であるため「個人情報の保存先」と記載しているが、基本的には利用者が利用するあらゆる情報の保存先となりうる全領域のことを意味している。

〔参考：パソコンの記録の仕組み〕

パソコンで利用者のデータの記憶処理を行う装置は、電源を落とすと記憶内容が消えるメモリと電源を落としてもデータが保存されるハードディスクがある。（図3 メモリとハードディスクでのデータの記録の仕組みを参照。）メモリは高速な読み書きが可能であり、ハードディスクはメモリよりも読み書きの速度は遅いが大きな記憶容量を持つという特長がある。パソコンの作業では、パソコンの起動後、ハードディスクに記録されたデータをメモリに読み出して作業を行い、作業終了時にはメモリにあるデータをハードディスクに保存し、パソコンの電源を落とすことが一般的である。作業後にパソコンの電源を落とすとメモリ上のデータは消える。

パソコンは、利用者が意図しない段階においても、メモリ上のデータをハードディスクに記録している。例えば、文書の編集作業の途中においても、停電などによってメモリ上のデータが消失することを防ぐためにソフトウェアが自動的に編集途上のデータをハードディスクに保存することがある。また、大きなデータをメモリに読み込んで処理を行う際には、一部のデータの退避先としてハードディスクが使われる。

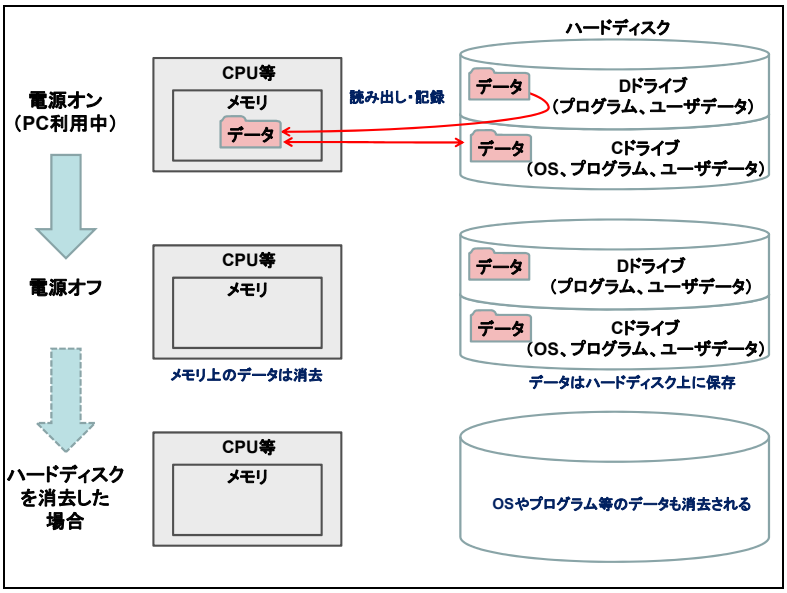


図3 メモリとハードディスクでのデータの記録の仕組み

（※なお、ハードディスクのドライブのパーティションの切り方は一例（以下同））

〔参考：ハードディスクの仕組み〕

ハードディスクには、利用者によって情報を保存することが可能な領域と、利用者が情報を保存しようとしても保存できない領域がある。（図4 ハードディスクの領域を参照。）前者はOS領域やデータ領域が、後者はOSの起動プログラムが格納されているマスターブートレコード（MBR）やパソコンベンダーが出荷時にインストールしたOSの復元用データを保存し、利用者から不可視に設定している領域等が該当する。また、一部の暗号化専用ソフトウェアでは、利用者がアプリケーションソフトを使用するOSを起動する前に、別のOS上で暗号化プログラムを起動してメモリ上に展開し動作させた後、利用者がアプリケーションソフトを使用するOSを起動するものがある。これらのOS起動前に動作するプログラムを格納した領域も利用者が利用する情報の保存先となりえない領域である。これらの利用者が利用する情報の保存先となりえない領域は、個人情報が書き込まれる可能性がないため「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」の対象とならない。

以上の説明のとおり、ガイドラインにおける「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」とは、ハードディスクのうち、ハードディスクの製造メーカやパソコンメーカのみが

使用する領域を除く全領域のことを指す。

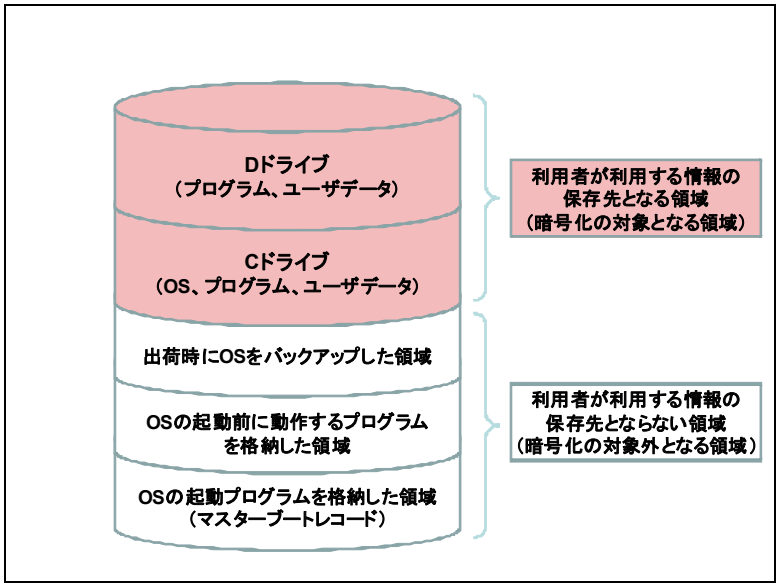


図4 ハードディスクの領域

＜個別条項Ⅰに該当する例（個人情報の保存先となる全領域が暗号化）＞

ⅰ 暗号化機能付き記録媒体

専用の暗号化チップにより、媒体上に書かれるデータがすべて自動的に暗号化、復号化されるため、個人情報の保存先として利用可能な領域のすべてが暗号化される。（ハードディスク、SSD（Solid State Drive：フラッシュメモリを利用した記録媒体）等において製品が販売されている。）

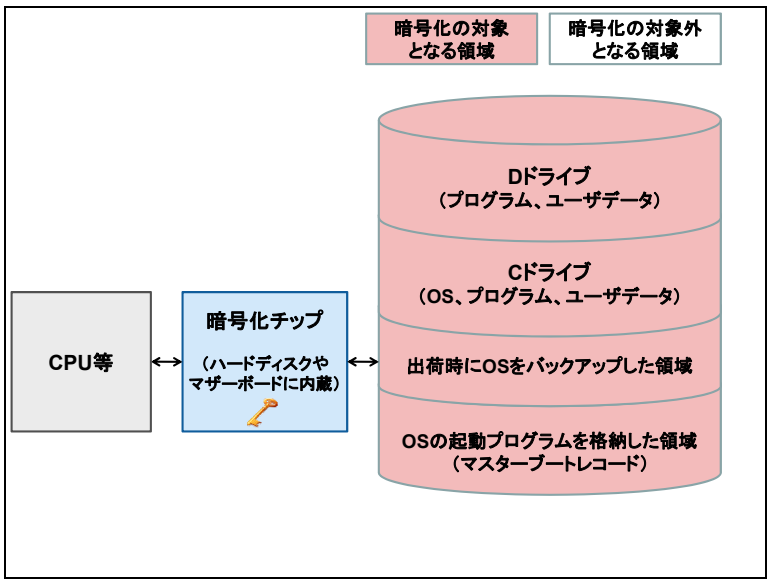


図5 ハードディスク全体の暗号化の例

ii　ディスク暗号化ソフトウェア

暗号化専用のソフトウェア（FDE SoftWare：Full Disk Encryption SoftWare）により、OSやプログラム、データがすべて自動的に暗号化、復号化される。暗号化ソフトウェアが格納された領域等、一部の領域は暗号化されないが、これらは個人情報の保存先として利用不可能な領域であるため問題はない。

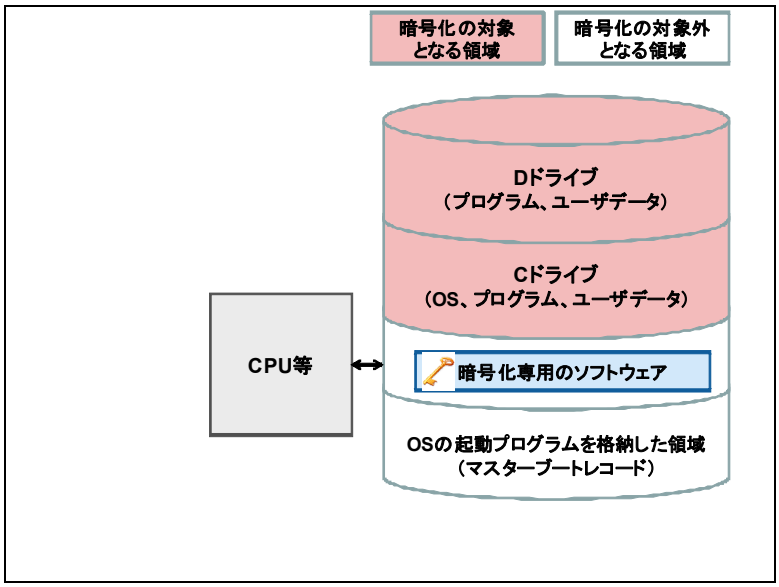


図6 ディスク暗号化ソフトウェアを用いた例

＜個別条項Ⅰに該当しない例＞

i　特定ファイルのみを指定した暗号化

OSが起動後、OS上のアプリケーションとして暗号化ソフトウェアが起動する場合で、暗号化したいファイルやフォルダを指定したうえで、その対象のみが暗号化される。暗号化処理を行ったファイルやフォルダ以外、通常のOS領域、データ領域が暗号化されておらず、一時データが暗号化されずに残っている可能性があるため、対象とならない。

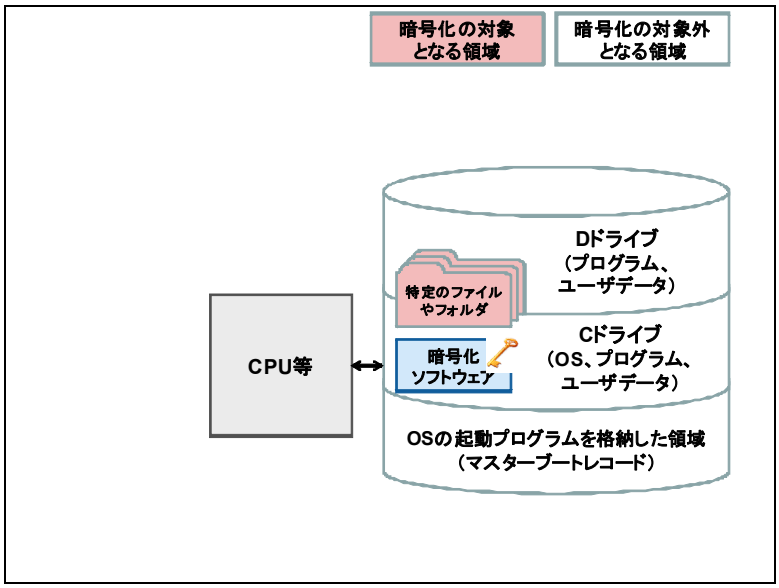


図7 特定のファイルやフォルダのみの暗号化の例

③「自動的に暗号化される」とは、ハードディスクへの書き込みが行われるたびにシステムが自動的に暗号化を行うことを指す。暗号化する際に利用者による個別の操作を必要とする場合、利用者が暗号化を忘却するリスクが存在するため対象とならない。

なお、「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」、また「自動的に暗号化」としなくとも、運用上の工夫によって個人情報を漏えいさせないことは可能であるが、利用者が意図せずに個人情報をパソコン内に保存してしまうことや、利用者が暗号化を忘却するリスク等もあるため、安全面を考慮し、全領域の暗号化、及び自動的な暗号化を条件としている。

Ⅱ　適切な暗号化された情報及び復号鍵の管理がされていること。

①次の（ア）又は（イ）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可能な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、②（ア）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、（イ）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。

（ア）次のA又はB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。

A　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。

B　③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、④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。

（イ）⑤遠隔操作により記録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、⑥記録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。

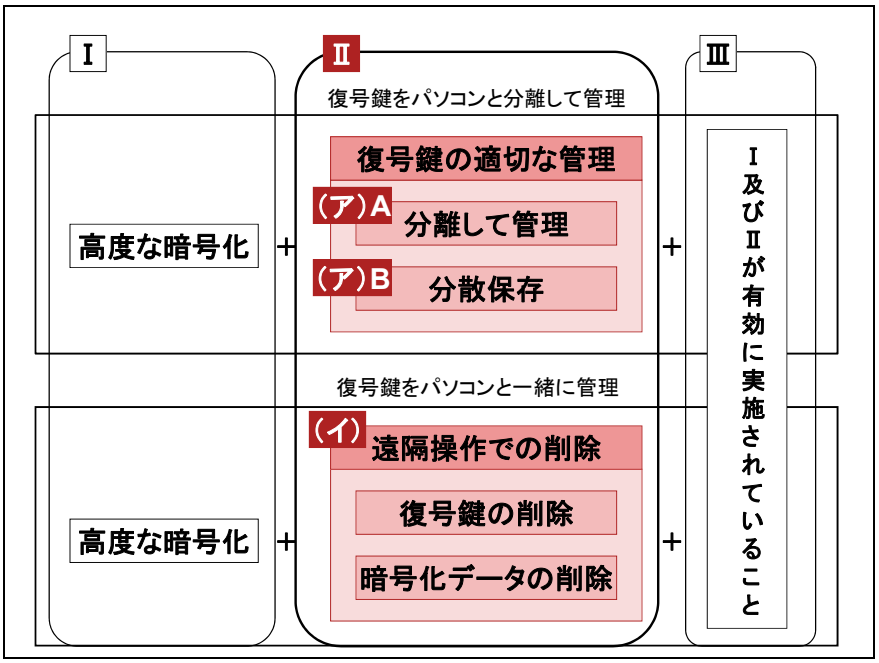


図 8 適切な安全管理措置の概要（Ⅱ　暗号化された情報及び復号鍵の適切な管理）

（解説）

① 上述したとおり、対象となる個人情報が高度な暗号アルゴリズムにより暗号化されていれば、一般には第三者がその個人情報を取得しても解読すること等は困難である。一方、高度な暗号化措置を施したとしても、鍵の管理が不十分な場合には、第三者に個人情報を解読されるおそれがあるため、暗号化された情報及びその鍵を適切に管理することが重要となる。

暗号化された情報及びその復号鍵の適切な管理とは、暗号化された情報と鍵を分離して管理する方法（ア）、及び暗号化された情報又は鍵（あるいはその両方）を第三者に解読される前に遠隔操作によって削除する方法（イ）が考えられる。

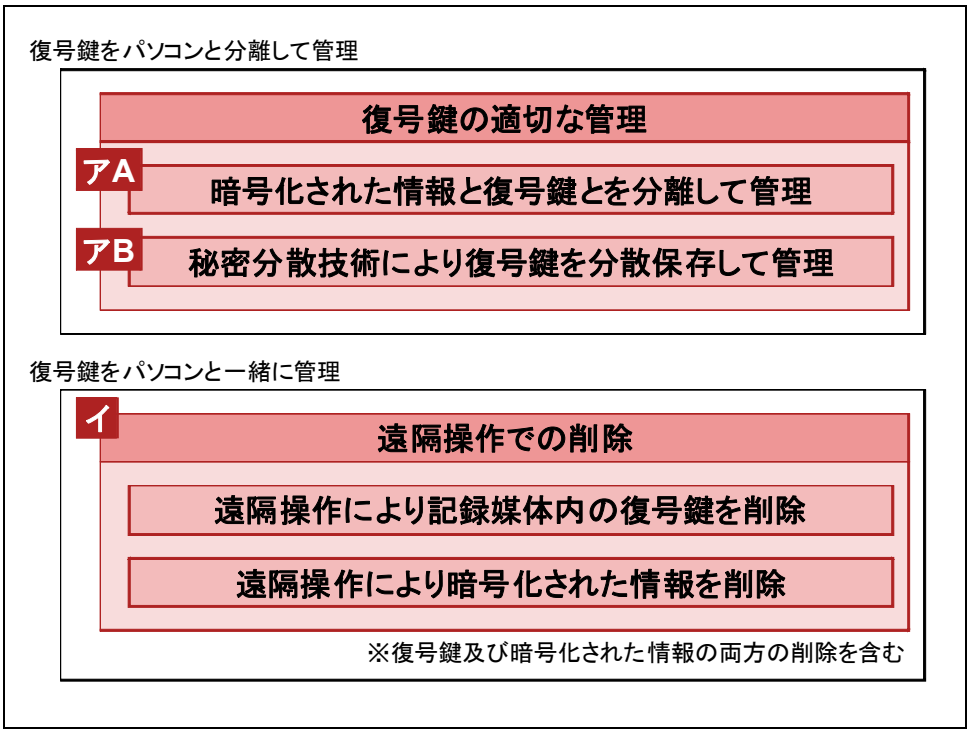


図9 暗号化された情報及び復号鍵の適切な管理

② 「（ア）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、」「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」とは、Aの方式については例えば、ⅰ ハードディスク等の個人情報の記録媒体とは分離独立したUSBメモリやICカード内の記憶領域に鍵を保存し、ⅱ USBメモリやICカード内の記憶領域に保存された鍵が個人情報の正当な所有者又は使用者以外の第三者によって読み取りや複製がされないよう措置（USBメモリやICカードにパスワードや指紋認証によるアクセス制限を設ける、又はパソコン及びUSBメモリやICカードにそれぞれ互いを特定する固有のIDや電子証明書を登録しておき、利用時に一対一対応を相互確認する相互認証機能を持たせる等）されており、ⅲ 又は復元キーワード等による代替鍵の生成と、それによる情報の復号化ができないよう措置されていることを指

す。

また、Bの方式については、ⅰ　情報を分散し、分散した個々の情報から元の情報を復元することを不可能とする秘密分散技術を用い、個人情報あるいは個人情報の暗号に用いた鍵を分散して保存し（例えば、一部をパソコンに格納、一部をUSBメモリに格納する等）、ⅱ分散保存された一部の情報を紛失したとしても、残りの情報が適正に管理されていること（第三者によって複製されていないことを含む）を指す。

一方、「（イ）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」とは、権限者以外の者が鍵を複製できないようにしていること、かつ権限者が複製したすべての鍵が適切な管理方法をもって管理されていること、又はハードディスク内の鍵を格納した領域に対して、権限者以外の者が、その領域外からアクセスし鍵を設定できない記録媒体（暗号化機能付ハードディスク等）を使用していることを指す。

＜（ア）Aに該当する例＞

ⅰ　パソコンを紛失したが、パソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っている場合。また、予備のUSBメモリがある場合は、その存在も確認できることが必要である。

＜（ア）Aに該当しない例＞

ⅰ　パソコンとパソコンのハードディスクに記録されたデータを復号するための鍵を格納したUSBメモリを同時に紛失した場合。また、USBメモリが手元に残っている場合でも、予備のUSBメモリが存在し、その存在が確認できない場合。

ⅱ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリは手元に残っているが、そのUSBメモリ内の鍵が容易に複製できた状態（例えば単純なファイルコピーや記憶領域全体の複製による）であり、複製が行われていないことを確認できない場合。

ⅲ　パソコンを紛失し、パソコンに記録されたデータを復号するための鍵を格納したUSBメモリが手元に残っているが、紛失したパソコンにおいて鍵とは異なる手段（例えば回避パスワードの入力）による復号化や、特定のキーワード入力による鍵の再生成が可能な場合。

〔参考：秘密分散技術（Secret Sharing）〕

秘密情報を分散して保存することにより秘匿性を実現する技術であり、分散した個々の情報から元の情報を復元することは不可能という特長がある。一般的には、情報（データ）そのものの分散ではなく、情報を暗号化した鍵の分散保存に用いられる。次の図10に示す例は、5個に分散された鍵データのうち3個を使って元の鍵が復元できる例である。

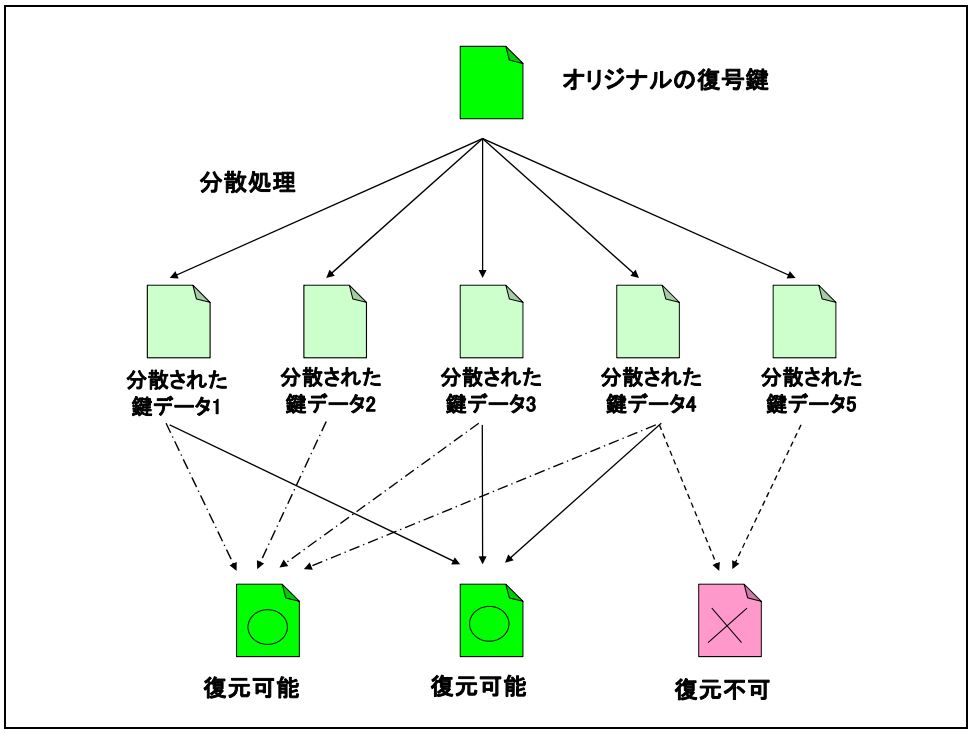


図10 秘密分散技術による鍵の分散管理

③ （ア）Bにおける「公知の方式」とは、秘密分散の方式が開示されており、第三者による検証が可能な方式を指す。さらには、第三者による評価論文等の入手が可能であることを指す。

また、「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」とは、方式が開示されており、複数の論文等で第三者による検証がなされている技術を指す。具体的には、所定の量の情報が無ければ多項式が解けないという性質を用いた閾値（しきい値）分散法が想定される。

④ Bにおける「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」の「当該復号鍵の構成部分」とは、パソコンに格納された分散された鍵データと、記憶媒体又はサーバに格納された分散された鍵データを指す。「紛失した暗号化された情報と分離されない構成部分」とは、パソコンに格納された分散された鍵データを指す。つまり、紛失したパソコンに格納された分散された鍵データのみではパソコンに格納された暗号化情報の復号ができないことを指している。

図 11 は、5個に分散された鍵データのうち3個を使って元の鍵が復元できる技術を利用する例である。5個の分散された鍵データのうち4個を外部記録媒体もしくはサーバに格納し、1個をパソコンに格納して利用した場合、パソコンには1個の分散された鍵データしかないため、パソコンを紛失したとしても、パソコンに格納された鍵データのみ用いて鍵を復元す

ることは不可能である。

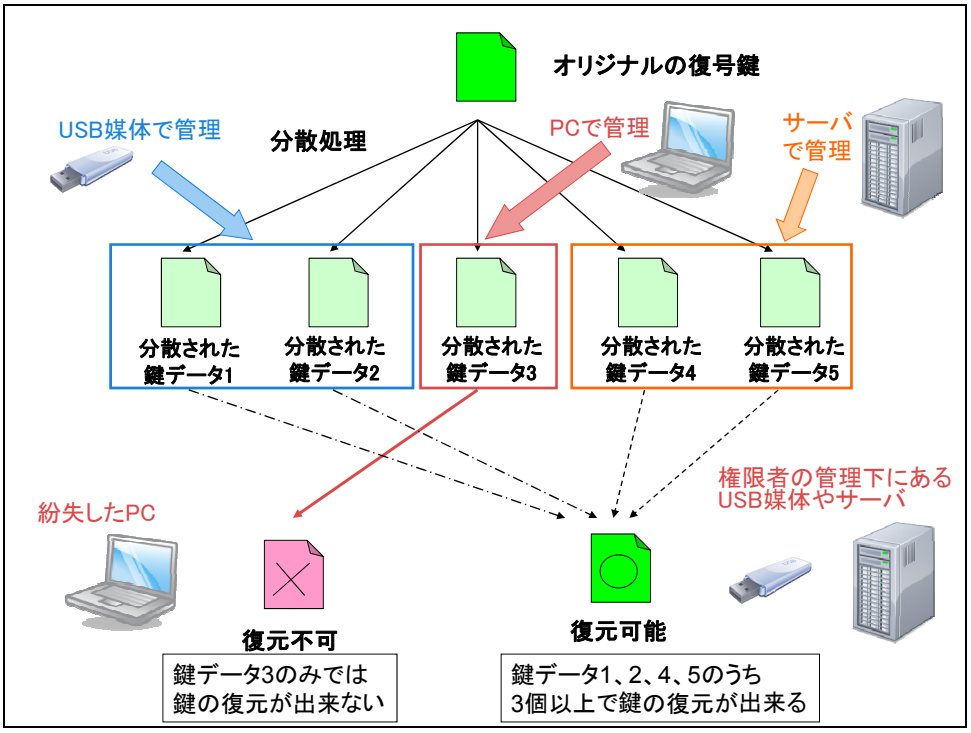


図11 秘密分散技術により鍵を分散管理する例

＜(ア)Bに該当する例＞

ⅰ 原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、当該パソコンに格納した分散された鍵データだけでは当該パソコンの暗号化された個人情報を復号できない場合であって、分散された鍵データの一部を格納したUSBメモリ等が手元に残っている場合。

ⅱ 原理的に部分復号が不可能な公知の方式を用いて鍵の分散管理を行い、パソコンは紛失したが、分散された鍵データの一部を権利者が管理するサーバ等に格納している場合等、紛失していない分散された鍵データが権利者の管理下にある場合。

＜(ア)Bに該当しない例＞

ⅰ 原理的に部分復号の可能性がある方式による秘密分散技術を用いた場合。例えば鍵を分散保持した場合に、分散保持された一部のデータより鍵の全体もしくは一部が推定される可能性のある方式を用いて鍵の分散管理を行ったパソコンを紛失した場合。

ⅱ 鍵の復元に必要な数の分散鍵データが権限者の管理下に無い場合。あるいは鍵の復元に必要な数の分散鍵データが紛失した場合。

⑤「遠隔操作により記録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」とは、パソコンが権限者の手元に無い状態であっても、ⅰ NIST 800-88(注1)で「Purging(実験室レベルでデータ復元不可能と定義)」に分類されている手法を適用して、記録媒体内の鍵又は暗号化された情報(あるいはその両方)を遠隔操作によって削除することあるいは、NIST 800-88でClearingに分類されている手法又は ⅱ JEITAの「パソコン廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」に則った手法を適用して、記録媒体内の暗号化された情報を遠隔操作によって削除することが想定される。

具体的には、Firmware Secure Erase Command(注2)により消去する(例:ATA(注3)準拠のハードディスクにおいてATA Security Erase Unit commandをモード指定して実行することにより、ハードディスク全体のデータを削除する、又は暗号化機能付きハードディスクの鍵を削除する)か(上記ⅰ)、専用ソフトにてハードディスク全体を固定パターン等にて一回以上、上書きすることによってデータを消去する(上記ⅱ)ことが想定される。

なお、削除とは記録媒体内の鍵又は暗号化された情報(あるいはその両方)の全体が消去若しくは書き換えられた時点を指す。

(注1) NIST 800-88: National Institute of Standards and Technology Special Publication 800-88 Guidelines for Media Sanitization.

(注2) Firmware Secure Erase Command: ハードディスク内のファームウエアによりセキュアに消去するためのコマンド

(注3) ATA: AT Attachment interface, ハードディスクの標準規格

⑥「記録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」とは、鍵又はデータを削除したことを示す完了レポートと、消去するまでの間にパソコンが使用されなかったことを権限者が確認できることを指す。

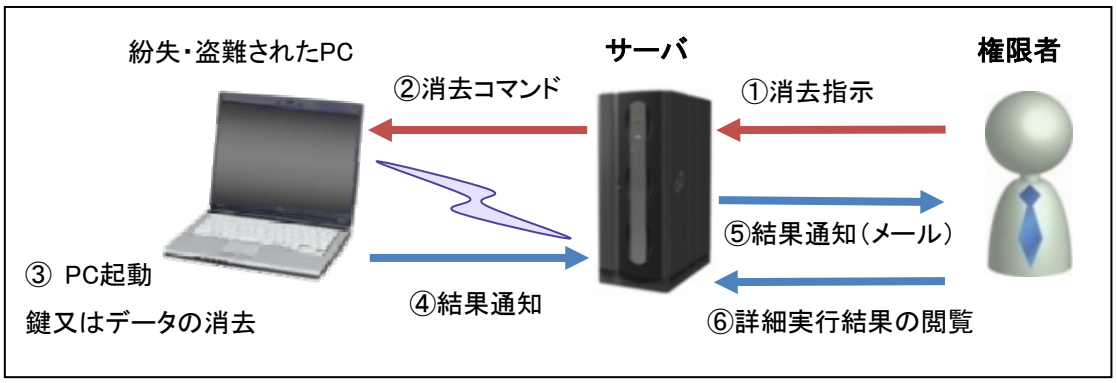


図12 鍵の複製、情報の閲覧、複写がされていないことを確認できる例

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

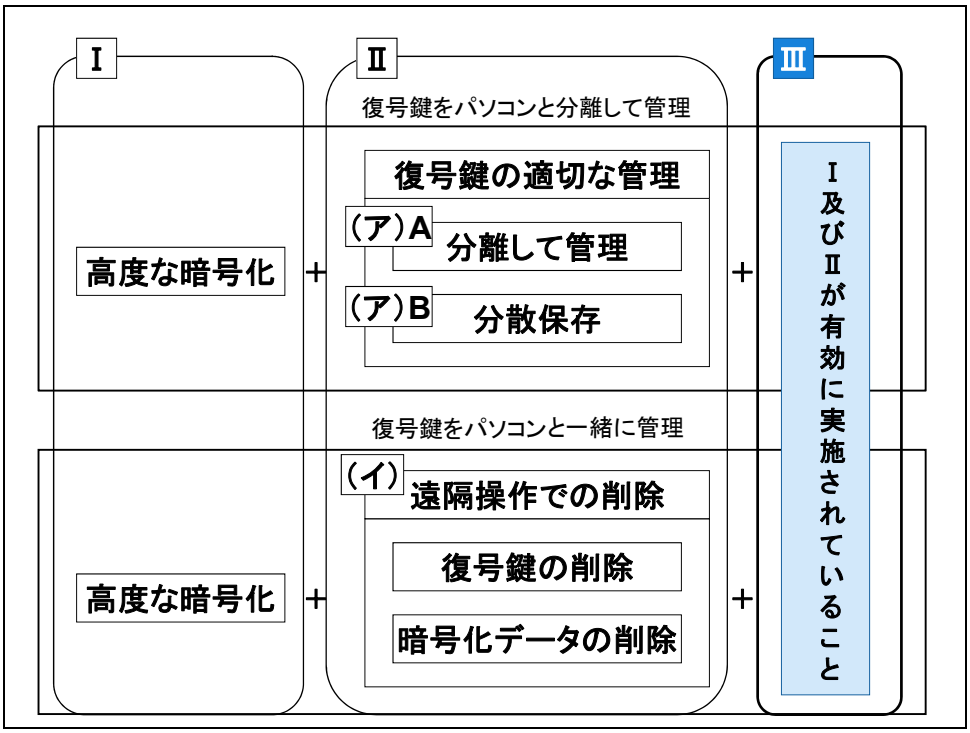


図 13 適切な安全管理措置の概要（Ⅲ 技術的保護措置の有効な実施）

（解説）

事業者において、Ⅰ及びⅡの技術的保護措置が実施されていたが、従業員による個別の設定変更によって当該機能が無効化されていた場合や、電源が入っており個人情報に容易にアクセス可能な状態でパソコンが盗難された場合等については、対象外となる。

また、紛失したパソコンのハードディスクドライブ上の鍵又は暗号化された情報（あるいはその両方）を権限者の遠隔操作によって削除できる機能を有する（Ⅰ及びⅡ（イ）を満たす）が、削除完了レポートによって、削除が完了するまでの間にパソコンが使用されたことを権限者が確認できた場合や、パソコンが通信圏外に持ち出された等の理由で削除完了レポートを権限者が受信できなかった場合等も対象外となる。

付録:

1. 電子政府推奨暗号(2003年度版)に記載されている共通鍵暗号

1)共通鍵暗号(64 ビットブロック暗号)

(1)3-key Triple DES

1979年に米国のFIPS認定されたDESの組合せ暗号である、鍵長168ビットの64ビットブロック暗号。1998年にNISTによりFIPS46-3として標準化され、ANSI X9.52としても規格化されている。SSL3.0/TLS1.0 に採用されている。

(2)MISTY1

1996年に三菱電機が発表した、鍵長128ビットの64ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

(3)Hierocrypt- L1

2000年に東芝が発表した、鍵長128ビットの64ビットブロック暗号である。

(4)CIPHERUNICORN-E

1998年に日本電気が発表した、鍵長128ビットの64ビットブロック暗号である。

2)共通鍵暗号(128 ビットブロック暗号)

(1)AES (Advanced Encryption Standard)

2001年に、Rijndaelをもとに、NISTがFIPS 197として標準化した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトにおいても、推奨アルゴリズムに選定されている。Rijndaelとは1998年にベルギーのJ.DaemenとV.Rijmen によりAESプロジェクトに提案され、2000年にAES Winnerに選定されたブロック暗号である。

(2)Camellia

2000年に発表された、NTTと三菱電機の共同開発による、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

(3)SC2000

2000年に発表された、富士通と東京理科大学の共同研究による、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。

(4)CIPHERUNICRON-A

2000年に日本電気が発表した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。

(5)Hierocrypt-3

2000年に東芝が発表した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号であ

る。

3）共通鍵暗号（ストリーム暗号）

（1）MUGI

2001年に日立製作所が発表した、鍵長128ビットのストリーム暗号である。

（2）MULTI-S01

2000年に日立製作所が発表した、鍵長256ビットのストリーム暗号である。

（3）RC4（128bit）

1987年にRSAセキュリティ社（当時RSAデータセキュリティ社）が発表した、鍵長128ビットのストリーム暗号である。SSL3.0/TLS1.0 に採用されている。CRYPTRECでは、128-bit RC4は、SSL3.0/TLS1.0 に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、可能な限りそちらを使用することが望ましい。また、RC4 は、SSL3.0/TLS1.0では鍵長40ビットと鍵長128ビットを選択して利用することが可能であるが、RC4を使うとしても、安全性確保の観点から、CRYPTRECとしては、鍵長128ビットで利用すべきであり、鍵長40ビットでの利用は避けるべきであると警告している。

2. ISO/IEC 18033シリーズに記載されている暗号

1）共通鍵暗号（64 ビットブロック暗号）

（1）3-key Triple DES

1979年に米国のFIPS認定されたDESの組合せ暗号である、鍵長168ビットの64ビットブロック暗号。1998年にNIST によりFIPS46-3として標準化され、ANSI X9.52としても規格化されている。SSL3.0/TLS1.0 に採用されている。

（2）MISTY1

1996年に三菱電機が発表した、鍵長128ビットの64ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

（3）CAST-128

Carlisle Adams、Stafford Tavaresらにより開発された64ビットブロック暗号である。鍵長は40ビットから128ビットの間の8の倍数である。秘匿通信のために使用するアルゴリズムとしてカナダ政府に認められた。CAST5ともいう。128ビットブロックに拡張したCAST-256はAES候補の一つであった。

2）共通鍵暗号（128 ビットブロック暗号）

（1）AES （Advanced Encryption Standard）

2001年に、Rijndaelをもとに、NISTがFIPS 197として標準化した、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号である。欧州の暗号評価事業であるNESSIEプロジェクトに

おいて、推奨アルゴリズムに選定されている。Rijndaelとは1998年にベルギーのJ.DaemenとV.Rijmen によりAESプロジェクトに提案され、2000年にAES Winner に選定されたブロック暗号である。

（2）Camellia

2000年に発表された、NTTと三菱電機の共同開発による、鍵長128ビット、192ビット、256ビットの128ビットブロック暗号。欧州の暗号評価事業であるNESSIEプロジェクトにおいて、推奨アルゴリズムに選定されている。

（3）SEED

1998年に韓国情報保護振興院（KISA)で開発されたブロック暗号である。韓国情報通信標準規格（KICS）、S/MIME（RFC4010）、SSL/TLS（RFC4162）、IPsec（RFC4196)の標準暗号として採用されている。

3）共通鍵暗号（ストリーム暗号）

（1）MUGI

2001年に日立製作所が発表した、鍵長128ビットのストリーム暗号である。

（2）MULTI-S01

2000年に日立製作所が発表した、鍵長256ビットのストリーム暗号である。

（3）SNOW 2.0

スウェーデンにより提案されたストリーム暗号である。

参考資料３

（参考資料３－１）

総務省「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」第二次提言（平成２２年５月）の抜粋

Ⅱ　ライフログ活用サービスに関する検討について
５．より信頼されるサービスに向けて（配慮原則の提言）
（ P.47～P.53 ）

（参考資料３－２）

総務省「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」第二次提言（平成２２年５月）の抜粋

Ⅲ　安全管理措置に関する検討について
２．想定されるリスクと技術的対応策
３．求められる安全管理措置
（ P.66～P.89 ）

（注1）参考資料3の引用文の頁は原文の頁のままです。
（注2）総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言の原文（全文）は総務省のホームページで公表されています。
http://www.soumu.go.jp/menu_news/s-news/02kiban08_02000041.html

参考資料３－１

利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会

第二次提言

（抜粋）

Ⅱ　ライフログ活用サービスに関する検討について

５．より信頼されるサービスに向けて

（配慮原則の提言）

平成２２年５月

５．より信頼されるサービスに向けて（配慮原則の提言）

これまで検討してきたとおり、ライフログ活用サービスは、その態様によっては、プライバシーを侵害し得るし、利用者の不安感等を惹起し得る。よって、ライフログを取得・保存・利活用する事業者は、利用者に対して一定の配慮をなし、円滑なサービスに資するための対策を取ることが望ましい。

事業者のなすべき配慮についてガイドライン等を行政が示すことも一手段として考えられる。しかし、ライフログ活用サービスは揺籃期にあり、事業者に過度の負担となってサービスの発展を妨げることは避けるべきであることから、まずは、規制色の強い行政等によるガイドラインではなく、事業者による自主的なガイドライン等の策定を促すべきであろう。よって、本研究会では、こういった自主的なガイドライン等の策定の指針となる緩やかな配慮原則を策定することとした。各業態[58]においては、本配慮原則を踏まえ、業態固有の事情を加味した自主的なガイドライン等を策定することが期待される[59]。

なお、ライフログ活用サービスが、今後、技術革新に伴って急速に発展することが想定されること、サービスのボーダレス性から国際的なハーモナイゼーションに対応する必要があること等から、定期的に本配慮原則を見直す必要がある。また、事業者による取組を促進するため、総務省において、本配慮原則を踏まえた事業者の取組を定期的に調査し、これを公表する必要がある。

（１）対象

①　対象情報

配慮原則の対象となる情報は、特定の端末、機器及びブラウザ等（以下「端末等」という。）を識別することができるものとする。対象情報は、個人情報保護法上の個人情報であるか否かを問わない。

例えば、クッキー技術等を用いて生成された識別情報、携帯電話端末に係るいわゆる契約者固有 ID、ログイン中の利用者を識別する ID、端末等のシリアル番号、MAC アドレスや IC タグの ID も、特定の端末等を識別することが可能であるから対象情報と

[58] 具体的には、現時点では、行動ターゲティング広告を配信する広告事業者、レコメンド機能を営む電子商取引サイト、ディープ・パケット・インスペクション技術を活用した行動ターゲティング広告を配信するインターネット・サービスプロバイダ、行動支援型サービスを行う携帯電話事業者等を想定している。

[59] FTC による「スタッフレポート：オンライン上の行動ターゲティング広告に関する自主行動原則」（FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising）も、事業者が自主的なガイドラインを作成するにあたっての根本的な原則であり、本配慮原則と同様のアプローチを採用している。

なる。また、これらと結びつけることが可能な閲覧履歴、検索履歴、購買履歴等の行動履歴も対象情報に含まれる。

前述したとおり、ライフログ活用サービスの提供に当たっては、個人識別性のない情報を取り扱う場面が多いと考えられる。個人識別性のない情報の取扱いについては、特定個人のプライバシーが侵害される場面は比較的限定されるとはいえ、プライバシー性が完全に失われていると考えるのは相当ではない。例えば、転々流通するうちに個人識別性を獲得してしまうおそれがあるし、大量に蓄積されて個人が容易に推定可能になるおそれがある。また、対象情報を取り扱う事業者にとっては個人識別性がないとしても、利用者本人にとって自らの情報であることが自明な情報については、その情報の取扱いに関与できないことが利用者の不安感等を惹起する可能性がある。

他方で、特定の端末等を識別することすらできない情報については、他の情報との照合や大規模な蓄積がなされたとしても、個人識別性を獲得する可能性は低く、プライバシー侵害の可能性は極めて低いと考えられる。また、特定の端末等を識別できない情報は、利用者本人にとっても自らの情報であることが判然としないため、利用者の不安感等は相当程度減じていると考えられる。

なお、対象情報が個人情報に該当する場合は、別途、個人情報保護法及び関係各ガイドラインの遵守が必要であることはいうまでもない。

② 対象事業者

対象となる事業者は、対象情報を事業（ただし、対象情報を蓄積せずに行う事業は除く。）の用に供している者とする。

「事業」とは、単に一定の目的をもって反復継続的に遂行される同種の行為であることだけでは足りず、社会通念上それが事業とみられる程度の行為であることを要する。例えば、個人でウェブサイトやブログを開設している場合では、対象情報が取得・保存・利活用されることもあるが、通常、電子商取引サイト等の事業を営んでいない限り、社会通念上事業とみられる程度の行為ではないことから、本配慮原則の対象となる事業者には含まれない[60]。

対象情報を蓄積せずに行うサービスについては、利用者の嗜好の分析の程度が低いこと、対象情報が保存されないことから、プライバシーが侵害されたり、利用者の不安感等が惹起されたりする場面は極めて限定的であり、配慮原則の対象としないこと

[60] もっとも、事業者ではない個人であっても大規模に対象情報を取得・保存・利活用している者も考えられる。こういった者は、対象事業者には含まれないとはいえ、自主的に配慮原則を踏まえたプライバシーポリシー等を整備することが望ましい。

が適当である[61]。

（２）配慮原則

具体的な配慮原則は以下の６つである。
① 広報、普及・啓発活動の推進
② 透明性の確保
③ 利用者関与の機会の確保
④ 適正な手段による取得の確保
⑤ 適切な安全管理の確保
⑥ 苦情・質問への対応体制の確保
以下、配慮原則の具体的な内容について説明する。

① 広報、普及・啓発活動の推進

対象事業者その他の関係者は、利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努めるものとする。

対象情報を取り扱う事業者その他の関係者に対し、広報、普及・啓発活動の推進に努めるよう配慮を求める原則である。本原則は、大きく分けると、利用者に対する広報、普及・啓発活動と、ライフログ活用サービス事業者への広報、普及・啓発活動で構成され、２つの広報活動が相まって利用者のリテラシーの向上や不安感等の払拭に資することが期待されている。なお、事業者以外の関係者としては、具体的には、消費者団体、公益法人、国や地方公共団体が考えられる。

１点目の利用者に対する広報活動についてであるが、これは後述する配慮原則「透明性の確保」の目的をより実効性のあるものにするために提言するものである。ライフログ活用サービスは、利用者から取得したライフログを利活用してサービスを提供するものであるが、プライバシー、個人情報保護の観点からすれば、ライフログを提供するかどうかは利用者の判断に委ねられるべきである。そして、その判断材料を提供するためには、サービスの仕組みについての透明性が確保されるべきである。そこで、本研究会では、透明性を確保すべく、事業者がサービスの仕組みについて利用者に明らかにするよう求めることとした（「②透明性の確保」を参照。）。

広報活動に係る本原則は、ライフログ活用サービスの認知度が低いことにかんがみ、事業者その他の関係者が、受動的にサービスの透明性を確保するのみならず、より積極的にサービスの仕組みについて利用者に広報、普及・啓発していくよう配慮を求め

[61] 対象情報を蓄積せずに行うサービスとしては、例えば検索連動型広告が挙げられる。（一般的に、検索連動型広告は検索キーワードを蓄積せずに行われている。）

ることにしたものである。

２点目の対象情報を取り扱う事業者への広報、普及・啓発活動についてであるが、ライフログ活用サービス事業者の中には、ライフログの取得・保存・利活用に当たって、利用者への配慮を行っていないか十分でない事業者が多数存在する。こういった事業者に対し、すでに配慮原則を踏まえたガイドライン等に基づいた取得等を行っている事業者やその他の関係者が、配慮原則について広報、普及・啓発を行うことによって、本配慮原則を踏まえたガイドライン等の普及を促し、ひいては利用者の不安感等の払拭に資することが期待される。

② 透明性の確保

対象事業者その他の関係者は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知り得る状態に置く（以下「通知等」という。）よう努めるものとする。通知等に当たっては、利用者が容易に認識かつ理解できるものとするよう努めるものとする。

前記のとおりライフログを事業者に提供するかどうかは利用者の判断に委ねられるべきである。その判断材料を提供するため、利用者関与の手段を含むサービスの仕組みについての透明性が確保されるべきである。本研究会では、透明性の確保を達成するために、事業者がサービスの仕組みについて利用者に明らかにすることを求めることとした。本原則は「③利用者関与の機会の確保」と相まって、事業者による対象情報の適正な取扱いを促すものであり、６つの原則の中核をなす。

なお、行動ターゲティング広告やレコメンドについては、国内外のガイドライン[62]や主要事業者の現状を基に検討した結果、少なくともア．取得の事実、イ．対象情報を取得する事業者の氏名又は名称、ウ．取得される情報の項目、エ．取得方法、オ．第三者提供の事実、カ．提供を受ける者の範囲、キ．提供される情報の項目、ク．利用目的、ケ．保存期間[63]、コ．利用者関与の手段について、利用者に通知し、又は知り得る状態に置くことが望ましい[64]と考えられる。

対象情報の取得・保存・利活用及び利用者関与の手段の詳細について通知等を行っていたとしても、それが利用者にとって認識されにくいか又は難解なものである場合には、透明性を確保するという本原則の趣旨が達成されないことになる。よって、通

[62] 我が国では「行動ターゲティング広告ガイドライン」（インターネット広告推進協議会　平成21年6月）が、アメリカでは”Self-Regulatory Principles for Online Behavioral Advertising“(American Association of Advertising Agencies et al. 2009年7月)がある。

[63] 保存期間には、端末等の識別を継続して行う期間と、蓄積した対象情報を保管する期限の２つがある。

[64] 一部の構成員から、どの広告が対象情報を活用した行動ターゲティング広告等なのか、利用者に容易に認識かつ理解できるようにすべきとの指摘があった。

知等に当たっては、事業者は利用者が容易に認識かつ理解できるものとすることが望ましい。

利用者が容易に認識かつ理解できる通知等の具体的内容については、例えば、取得者のプライバシーポリシー等を掲載したページに、取得事実等を簡潔かつ目を惹きやすい形で掲載することを念頭に置いている。

行動ターゲティング広告においては、第三者による対象情報の取得や広告やウェブビーコンの配信が行われる場合等、広告の掲載者と対象情報の取得者や広告等の配信者とが異なる場合が考えられ、対象情報の取得者や広告等の配信者のウェブサイトに取得事実等を単純に表示しても、利用者が確認することが困難であり、透明性を確保したことにはならないのではないかという問題がある。この場合は、広告の掲載者のウェブサイトにおいて、第三者による対象情報の取得や広告等の配信が行われていることを明示した上で、取得者の名称、取得事実等に係る情報が掲載されたページへのリンクをはることが望ましい[65]。

③　利用者関与の機会の確保

対象事業者は、その事業の特性に応じ、対象情報の取得停止や利用停止等の利用者関与の手段を提供するよう努めるものとする。

対象情報に関して誤った取扱いがなされることに起因するプライバシー侵害や個人情報の不適切な取扱いを予防・是正する観点から、事業者に対し、対象情報を最もよく知り得る立場にある利用者が情報の取扱いに関与できる手段を提供するよう求める原則である。この原則は、透明性の確保の原則が適切に実現されていることが前提となる。

現在、行動ターゲティング広告では、行動ターゲティング広告配信停止手段[66]の提供が広く行われている。通常、この手段の提供は、行動ターゲティング広告の配信を拒否したブラウザであることを示すクッキー（オプトアウトクッキー）を発行することにより行われている。ただし、この手段は、クッキーが削除された場合にオプトアウトが解除されてしまうものであり、異なるブラウザの利用、端末の買換え、OS の再インストールの場合等に、再度、クッキー発行の手続をとることが必要となる一定の制約がある。事業者には、オプトアウトクッキーの制約について利用者に説明することが求められる。

---

[65] 第三者による対象情報の取得及び広告の配信については、プライバシーへの影響度合いが大きいため、どのウェブサイト上において行われているかを対象情報の取得者が明らかにすべきとの指摘があった。

[66] 通常、行動ターゲティングされた広告の配信が停止され、その代わりに行動ターゲティングされていない広告が配信される。

他には、プライバシーポリシー等のページで、クッキーの拒否、クッキーの削除について説明するとともに、その設定方法を掲載しているウェブサイトが散見される。クッキーの拒否、削除によりブラウザを識別することが出来なくなるため、取得情報は対象情報からはずれることになるとはいえ、通常のブラウザの設定では、個別のクッキーを拒否することが難しいことも考慮される必要があると思われる[67]。

また、携帯電話インターネットでは、契約者固有 ID の非通知について説明するとともに、その設定方法を掲載しているウェブサイトが散見される。契約者固有 ID の非通知により、同様にブラウザを識別することが出来なくなり、取得情報は対象情報からはずれるとはいえ、契約者固有 ID が非通知になっていると利用できないサイトやサービスが広く存在することも同様に考慮の必要があると思われる。

以上からすれば、結局、事業者は上記の行動ターゲティング広告配信停止手段の提供、クッキーの拒否・削除等の利用者関与の手段を、事業の特性に応じて総合的に提供することが求められる。「事業の特性に応じ」としたのは、ライフログ活用サービス事業者の事業は多種多様であり、利用者関与の手段も、その特性に応じて柔軟に提供されるべきだからである。

事業者には、今後、簡便に利用者が対象情報の取扱いを確認し、取得及び利用を停止させる手段を提供することが望まれる[68]。

④ 適正な手段による取得の確保

対象事業者は、対象情報を適正な手段により取得するよう努めるものとする。

不正手段による取得には、取得者や取得情報の範囲等を偽る場合（通常人が想定する範囲を大きく逸脱して取得される場合を含む。）、利用者が全く認識し得ない手段を用いる場合等が考えられ、かかる態様の取得に対する利用者の不安感等が高まっている。こういった事案に対応し、不安感等を払拭し、対象情報の適正な取扱いに対する利用者の信頼を確保する観点から、取扱いの起点である取得段階から適正性が確保されていることが重要である。よって、対象情報を適正な手段により取得するよう提言するものである。

具体的な適正性の判断については、ケースバイケースであり、各法令の趣旨や社会通念に委ねられる。

---

[67] この手段によると、例えば、Windows Internet Explorer 8 は、個別のクッキーを拒否するための機能を標準で用意している。また、Mozilla Firefox バージョン 3.0 系列や Google Chrome 4.0.249.89 ではアドオンを追加することによって個別のクッキーを拒否することが可能になる。

[68] 一部の構成員から、簡便に利用者が対象情報の取扱いを確認し、取得及び利用を停止させることが可能な技術的手段の発展が望まれるとの指摘があった。

⑤　適切な安全管理の確保

対象事業者は、その取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要かつ適切な措置を講じるよう努めるものとする。

対象情報が、不正に取得した者によって利用に供された場合、プライバシーの重大な侵害が惹起される場合が考えられる。このため、対象情報を取得した事業者に対し、その取り扱う対象情報が漏えい、滅失又はき損の危険にさらされることのないよう配慮を求めるものである。

⑥　苦情・質問への対応体制の確保

対象事業者は、対象情報の取扱いに関する苦情・質問への適切かつ迅速な対応に努めるものとする。

対象情報の取扱いをめぐるトラブルは、基本的に私人間の問題であるため、まずは当事者間で話し合うことで迅速な解決を図ることが望ましい。このため、事業者に対し、対象情報の取扱いに関する苦情や質問に対応する窓口を設け、適切かつ迅速な処理に努めるよう配慮を求めるものである。

参考資料３－２

利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会

第二次提言

（抜粋）

Ⅱ　安全管理措置に関する検討について

２．想定されるリスクと技術的対応策

３．求められる安全管理措置

平成２２年５月

２．想定されるリスクと技術的対応策

（１）想定されるリスク

モバイル PC 等により個人情報を社外に持ち出す場合に生じ得るリスクとしては、大きく分けて、①モバイル PC 等が権限のない者に使用されることによる漏えいリスク、②モバイル PC の記録媒体を物理的に取り出されることによる漏えいリスク、③ネットワーク上を流通する情報を盗み取られることによる漏えいリスクの３つが考えられる。

① モバイル PC 等が権限のない者に使用されることによる漏えいリスク

持ち出したモバイル PC 等が紛失、盗難にあった場合に、権限のない第三者に使用されることにより、そのモバイル PC 等の中に記録された情報を閲読されるおそれがある。また、モバイル PC に社内データベースへのアクセス権限が付与されている場合には、社内データベース上の情報まで閲読されるおそれがある。

② モバイル PC の記録媒体を物理的に取り出されることによる漏えいリスク

モバイル PC の内部にあるハードディスク等の記録媒体に情報を記録する場合には、その記録媒体を物理的に抜き出されることにより、他の PC に接続して情報を読み出されるおそれがある。

③ ネットワーク上を流通する情報を盗み取られることによる漏えいリスク

ネットワーク上で情報のやりとりをする場合には、ネットワーク上を流通する情報を盗み取られることにより、その内容を閲読されるおそれがある。例えば、電子メール等でのやりとりや、社内ネットワーク内に存在するデータへのアクセスなどの場合に、このようなリスクが生じることになる。

（２）リスクに対応する技術的保護措置

以上のようなモバイル PC 等により個人情報を社外に持ち出す場合に生じ得るリスクに対応するために用いることができる技術がある。具体的には、個人認証技術、暗号技術、シンクライアント、遠隔データ管理である。

① 個人認証技術

個人認証技術とは、本人のみが持ち得る情報等を用いて、本人であることを確認するための技術である。この技術を導入することで、モバイル PC 等が権限のない者に使用されることによる漏えいリスクに対応することができる。

個人認証技術を導入可能な部分としては、BIOS（Basic Input / Output System）等のハードウェアの起動時、オペレーティングシステム（Operating System : OS）やアプリケーション等のソフトウェアの起動時がある。これらの複数の段階で導入することも可能であり、その場合には、セキュリティ強度は、より強固なものとなる。

個人認証技術による認証方法としては、パスワード等の記憶により本人（利用者）を識別する方法、IC カード、USB（Universal Serial Bus）キー等の所有物により本人を識別する方法、静脈、指紋、顔等の生体情報により本人を識別する方法の３方式がある。これらの認証方式には、それぞれメリット・デメリットが存在する。

ア 記憶による認証

記憶による認証は、専用のハードウェアが不要である等、導入が容易という利点がある。一方で、パスワード等を忘却したり他人に教えたりするという本人による不適切な管理が起こりやすいという欠点や、桁数が少ないパスワードや辞書等に記載されている単語の組合せによるパスワードの場合等は、第三者に類推されるおそれがあるという欠点が指摘されている。また、長く類推されづらいパスワードになるほど、本人が忘却する可能性が高くなるという問題がある。

イ 所有物による認証

所有物による認証は、その所有物でなければ認証に成功しないことから、唯一性が高いという利点がある。また、記憶による認証と比べて忘却する可能性は低いという利点もある。導入の容易さについても、多くのノート PC には標準で USB ポートが搭載されているなど、媒体の選び方によっては、容易に導入することも可能である。その一方で、ノート PC とともに紛失、盗難にあった場合には、容易に認証を破られるという欠点が指摘されている。

ウ 生体情報による認証

生体情報による認証は、忘却や紛失、盗難のおそれがないという利点がある。一

方で、精度の設定次第では他人を受け入れてしまったり、本人を拒絶してしまったりするという欠点がある。生体情報による認証の中でも、指紋認証や静脈認証では、他人受入率が 0.001%～0.00001%程度であるのに対して、声紋認証や顔認証等では、他人受入率が 1%～0. 1%と相対的に高くなっている。また、一度登録した生体情報は本人が生涯変更することができないため登録情報の厳格な管理が求められるという留意点が指摘されている。

表３　個人認証方法とその特徴

	利点	欠点	認証の強度	利用形態	備考
記憶による認証					
パスワード	導入が容易	忘却、漏えい、類推等	管理・設定方法に依存	専用のハードウェア不要	BIOS、OS、アプリケーションソフトウェア等で対応
所有物による認証					
接触／非接触型ＩＣカード	唯一性が高い 忘却の可能性が低い	紛失、盗難等	情報とともに紛失、盗難に遭うと弱い （PIN併用で、強度向上）	PC内蔵/PC外付けのリーダライタ	交通系カード、携帯電話などで利用可能
USBキー	〃	〃	〃	USB インターフェース	ほとんどのPCにはUSB インターフェースが標準搭載
生体情報による認証					
指紋認証	忘却等のおそれがない	荒れた（磨耗した）指紋では認証率が低下	他人受入率:1/10万～1/1000万(※)	PC内蔵/PC外付けセンサ	PCによっては、センサーを標準搭載
静脈認証	忘却等のおそれがない 体内情報で偽造困難	直射日光下では認証率低下	他人受入率:1/10万～1/1000万(※)	PC外付けセンサ	銀行ATMで用いられている実績
顔認証	忘却等のおそれがない	照明変動、姿勢変動に弱い	他人受入率:1/100(※)	PC内蔵/外付けのWebカメラ	主にデジカメの顔識別で実績
声紋認証	忘却等のおそれがない	風邪、喉の酷使後の声質変化に弱い	他人受入率:1/100(※)	PC内蔵/外付けのマイク	電話による本人認証で実績

（※）認証の強度は、一般的なものであり、使用状況によって異なる

② 暗号技術

ア 暗号技術の動向

暗号技術とは、保護対象の情報について特定情報を用いて変換を施すことにより（暗号化）、その変換された情報を、特定情報を用いて元に戻さなければ（復号）、保護対象の情報の内容を知り得ないようにする技術である。

暗号技術では、暗号化に用いられる特定情報（暗号鍵）と復号に用いられる特定情報（復号鍵）で異なる鍵を用いる公開鍵暗号方式と、暗号鍵と復号鍵で同一の鍵を用いる共通鍵暗号方式がある。

現代社会では、インターネットでのショッピング、携帯電話での通信、地上デジタル放送の受信、電子メールへの電子署名等様々な場面で暗号技術が用いられている。

図５ 暗号技術の用いられる場面

暗号アルゴリズムについては、いくつかの公的機関が、その安全性等について客観的評価を行った上で、使用が推奨されるものを公表している。また、暗号アルゴリズムについては、解読技術の発展、コンピュータ能力の向上等によって、強度が弱くなる（危殆化が生ずる）ことから、不断に検証が行われており、より強度の高い暗号アルゴリズムへの移行スケジュールの公表や推奨の停止等が行われている。

国内では、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである CRYPTREC（Cryptography Research and Evaluation Committees）において、電子政府推奨暗号リストを公表している。また、暗号技術に関する国際標準規格としては、ISO（国際標準化機構（International Organization for Standardization））・IEC（国際電気標準会議（International Electrotechnical Commission））の策定した、ISO/IEC 18033 が存在する。その他、

米国をはじめとした諸外国でも、公的機関により、推奨される暗号アルゴリズムが公表されている。

表４　公的機関で客観的な評価・公表が行われている暗号アルゴリズム

	電子政府推奨暗号 （平成15年度版）(1)	ISO/IEC 18033シリーズ	NIST SP 800-57 （2030年末期限の場合）
	公表元：総務省，経済産業省 原案策定：CRYPTREC (2)	国際標準規格 策定：ISO/IEC JTC 1/SC27 (3)	策定：米国立標準研究所
公開鍵暗号			
署名	RSA-PSS(1024bit)、 RSASSA-PKCS1-V1_5(1024bit)、 DSA(1024bit)、ECDSA(160bit)	記載なし（ISO/IEC 9796-2等で規定）	RSA(2048bit)、DSA(2048bit)、 ECDSA (224bit)
守秘	RSA-OAEP(1024bit)、 RSAES-PKCS1-V1_5(1024bit)	RSA-KEM、RSA-OAEP、 PSEC-KEM、ACE-KEM、 HIME(R)、ECIES-KEM	推奨なし
鍵共有	PSEC–KEM (160bit)、 DH(1024bit)、ECDH(160bit)	記載なし（ISO/IEC11770-3で規定）	DH、MQV
共通鍵暗号			
64 bitブロック暗号	3-key TDES、MISTY1、Hierocrypt-L1、CIPHERUNICORN-E	TDES(3-key推奨)、 MISTY1、CAST-128	3-key TDES
128 bitブロック暗号	AES、Camellia、SC2000、 CIPHERUNICRON-A、Hierocrypt-3	AES、Camellia、SEED	AES
ストリーム暗号	MUGI、MULTI-S01、RC4(128bit)	MUGI、MULTI-S01、 SNOW 2.0	推奨なし
ハッシュ関数			
	SHA-256、SHA-384、SHA-512、 SHA-1、RIPEMD-160	記載なし（ISO/IEC 10118 で規定）	SHA-224、SHA-256、 SHA-384、SHA-512

※　表中にあるそれぞれのアルゴリズムには、期限や条件が付されているもの等もあるため、実際に利活用する場合には、原典を確認すること
(1) 平成25年度から新たな推奨暗号の体系に移行することから、現在、リスト見直しのための検討が行われている
(2) CRYPTREC：Cryptography Research and Evaluation Committees　　事務局（総務省、経済産業省、NICT、IPA）
(3) ISO / IEC Joint Technical Committee 1 / SubCommittee 27 "IT Security techniques"
ISO：International Organization for Standardization（国際標準化機構）、IEC：International Electrotechnical Commission（国際電気標準会議）

イ　情報の暗号化

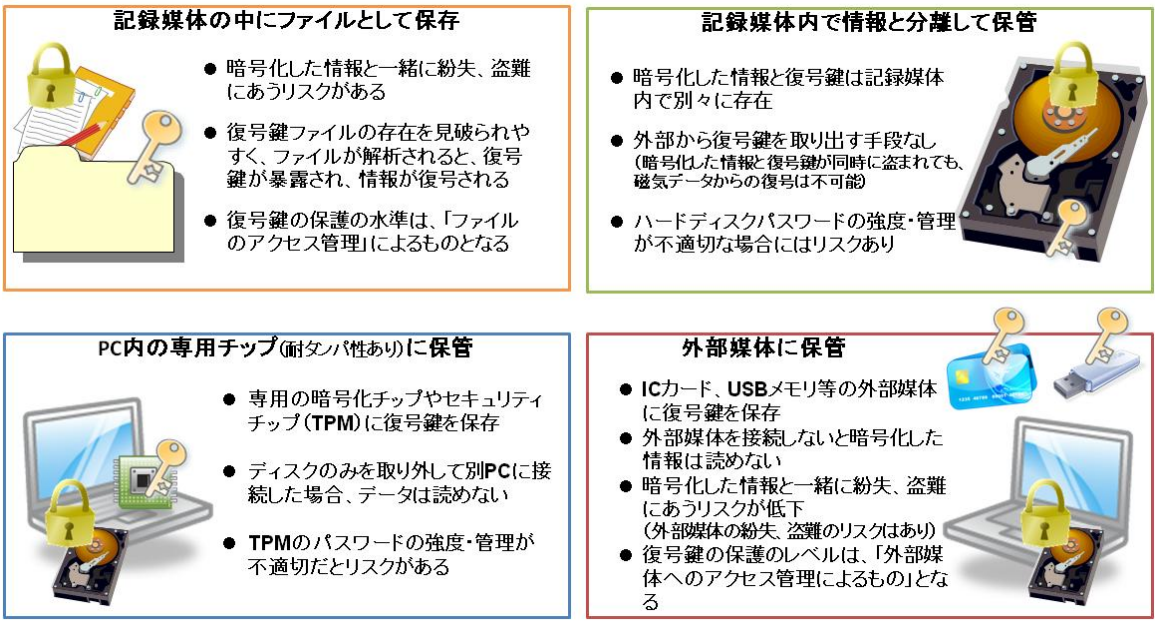
モバイル PC 等により社外に持ち出す情報を適切な暗号アルゴリズムを用いて暗号化することにより、モバイル PC の内部にある記録媒体を物理的に抜き出されることによる漏えいリスクに対応することができる。また、ネットワーク上でやりとりするファイルを適切な暗号アルゴリズムを用いて暗号化することにより、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクにも対応することができる。

暗号技術で重要となる復号鍵の管理については、暗号化した情報が存在する記録媒体の中に保存する方法では、記録媒体と一緒に紛失、盗難に遭うため、復号鍵を盗みだそうとする攻撃から守ることのできる耐タンパ性を持ったモバイル PC 等の中の独立したチップ上で管理する方法、IC カード等の別の媒体で管理する方法等、より適切に管理する方法がある。

復号鍵の適切な管理がなされている場合には、暗号化した情報が存在する記録媒体が紛失、盗難に遭ったとしても、第三者が復号鍵を手に入れることができないため、情報の内容を知られる可能性は極めて低い。

なお、暗号化する対象としては、個々のファイル、特定のフォルダなど記録媒体の特定の領域、記録媒体全体等が考えられる。

図６　復号鍵管理の方法



ウ　通信経路での暗号化

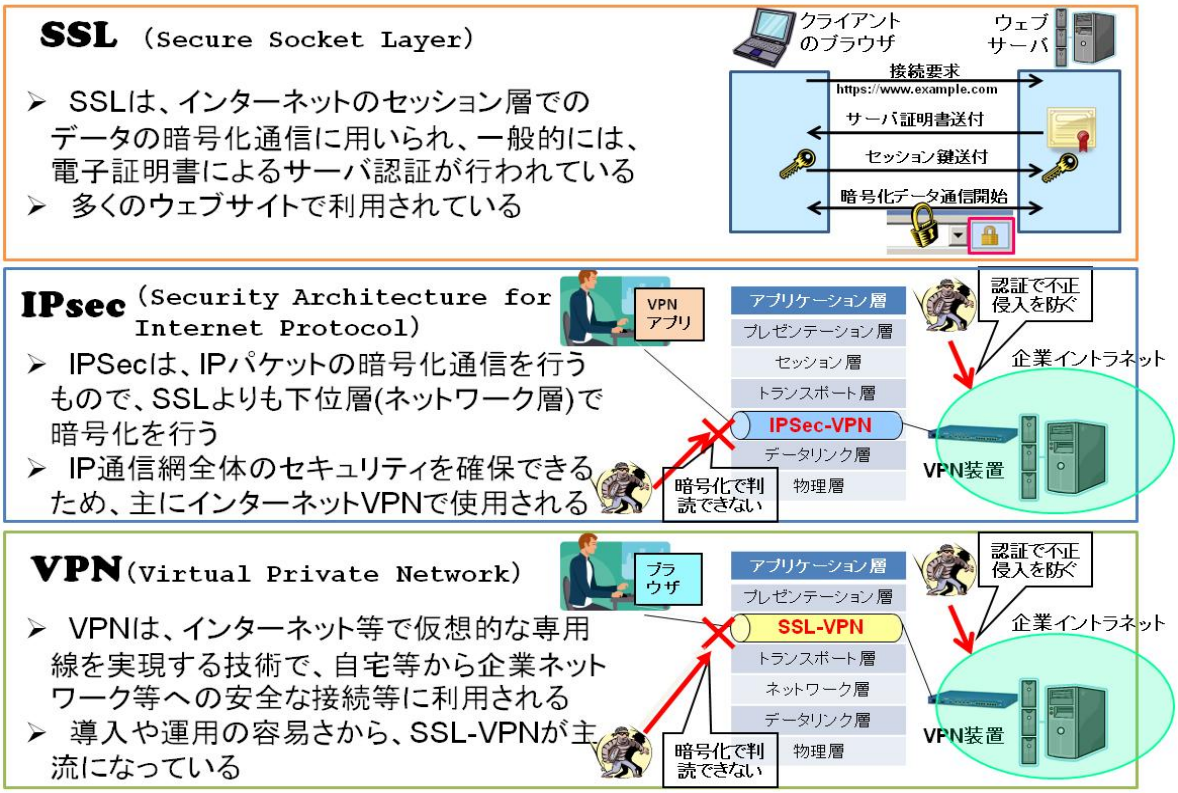
通信経路を暗号化することにより、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクに対応することができる。

通信経路での暗号化方法としてはさまざまなものがあり、その中で代表的な方法としては、SSL（Secure Socket Layer）、IPsec（Security Architecture for Internet Protocol）が挙げられる。

SSL は、一般的には証明書によるサーバ認証が行われるものであり、電子商取引や個人情報等の秘匿性のある情報のやりとりをするウェブサイトの多くにおいて利用されている。IPsec は、IP パケットの暗号化通信を行うものであり、セッション層において暗号化を行う SSL よりも下位層の IP 層において暗号化を行うものである。

VPN（Virtual Private Network）は、SSL 等による暗号化通信を行うことで、仮想的な専用線を実現する技術であり、自宅等の外部から企業ネットワーク等に安全に接続する場合等に利用される。

図７　通信経路での暗号化

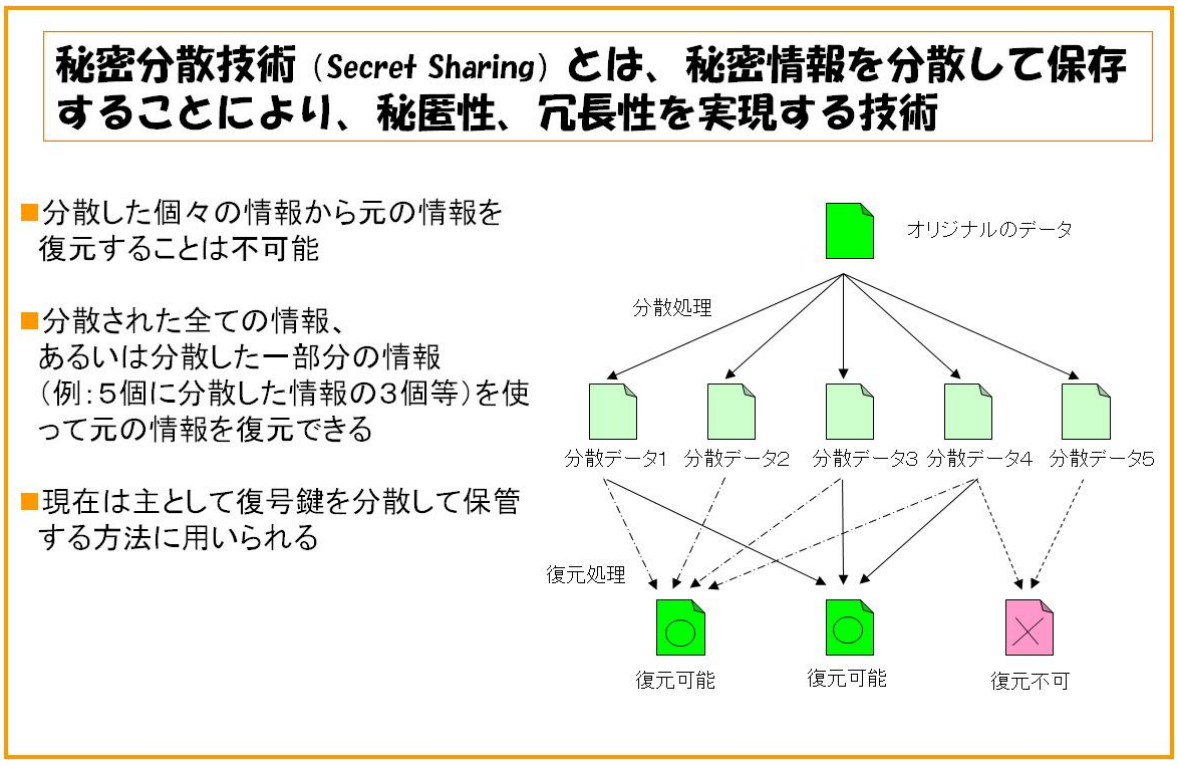


③　秘密分散技術

秘密分散技術（Secret Sharing）とは、秘密情報を分散して保存することにより、秘匿性、冗長性を実現する技術である。分散した個々の情報から元の情報を復元することは不可能で、分散された全ての情報、あるいは一部分の情報を使って元の情報を復元できる特長がある。なお、分散された各々の情報の大きさは、理論上、元の情報の大きさと同じである。また、分散された情報に復元処理に必要な情報が添付されている場合は元の情報よりも大きくなる。

秘密分散技術の応用により、複数の記憶媒体やネットワーク上のサーバに個々の分散した情報を保存し、盗難や漏えい及び災害や故障に対する安全性を保つことが可能である。また、分散した情報の一部をネットワーク上のサーバや、USB メモリ、IC カード等の他の媒体に格納することも可能である。現在は、主として復号鍵を分散して保管するために用いられることが多い。

図８　秘密分散法



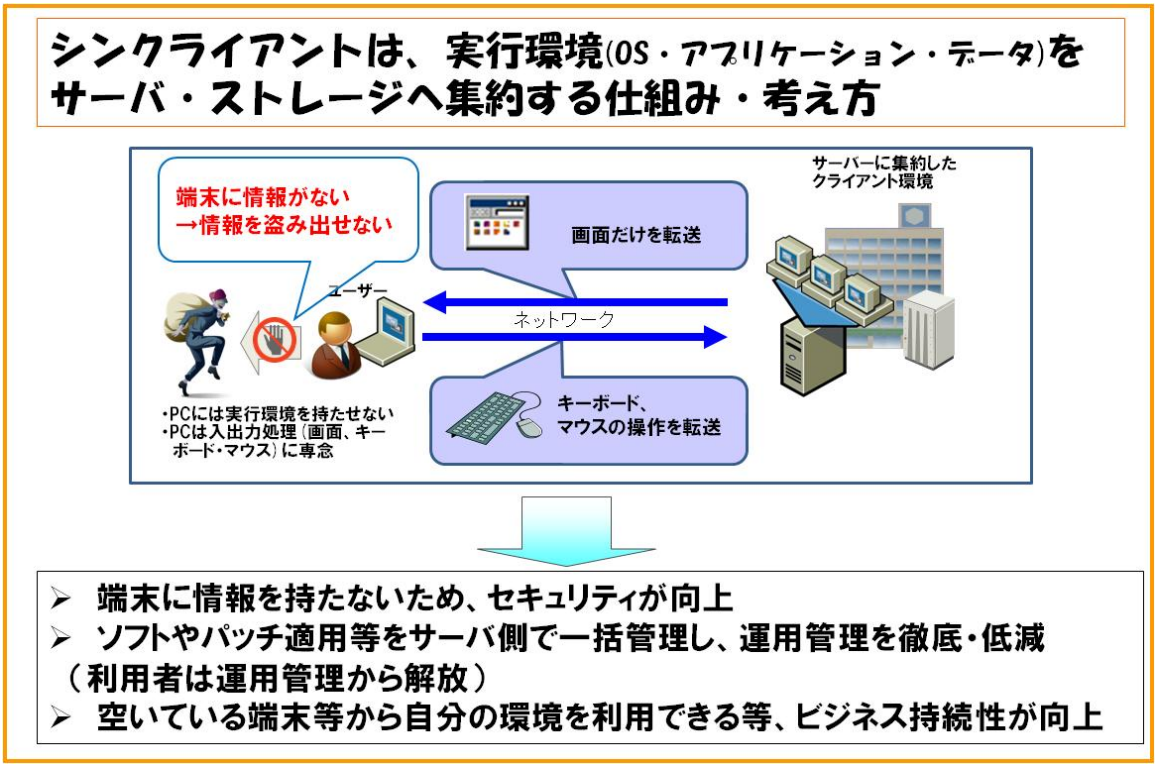
④　シンクライアント技術

シンクライアント技術とは、従業員等が使用する利用者側端末（クライアント）には最小限の機能（ネットワーク機能、画面表示・操作機能）のみを持たせ、アプリケーションやデータはサーバ側で管理する技術である。

シンクライアント技術により、利用者側端末の記憶媒体を物理的に取り出されることによる漏えいリスクに対応することができる。一方で、サーバと利用者側端末との間で情報が伝達されることになり、盗聴されにくくする配慮はなされているものの、不可能ではないため、通信経路の暗号化等による適切な対応が必要である。

なお、シンクライアント技術には、主に、サーバでアプリケーションを実行し、その画面情報を利用者側端末に転送する方式と、サーバにある OS やアプリケーションを実行するためのデータを利用者側端末に転送し、データ処理を利用者側端末で行う方式がある。前者の方式は、サーバの画面情報の転送であり、利用者側端末で処理が行われないため、情報漏えいのリスクは低いが、転送する情報量が多くなる。後者の方式は、データ処理を利用者側端末で行うため、転送する情報量は相対的に少ないが、利用者側端末でのデータ処理に際して情報が記録されることになるため、情報漏えいのリスクは相対的に高くなる。このため、採用するシンクライアント技術の方式に合わせて、適切なリスク管理が必要である。

図９　シンクライアント技術（画像転送方式）



⑤　遠隔データ管理技術

社外に持ち出したモバイル PC に対して、専用のソフトウェアやハードウェアによって遠隔操作する様々な仕組みも存在する。これらは、携帯電話や Wi-Fi 等の通信網を用いて、モバイル PC のアプリケーションや BIOS 等に対して指示を出すものである。

例えば、モバイル PC が紛失、盗難にあった場合に、そのモバイル PC の機能を制限したり、起動できないようにしたりすることや、内部の情報や暗号化された情報の復号鍵を削除し、第三者に閲読されることがないようにすること等が可能となる。この場合には、指示を出した者がそれらの措置の実行結果を把握可能とするサービスも存在する。

また、モバイル PC の位置情報を管理し、紛失、盗難時に発見に向けた対応を可能にするようなサービスも存在する。

なお、これらの遠隔データ管理技術では、対象となるモバイル PC が通信圏外に持ち出された場合には、遠隔操作ができないことや、遠隔操作結果を得られないことがある。このため、サービスによっては、断続的な指示の送信や、圏外での起動抑止等の補完的な対応が取られている。

図 10　遠隔データ管理技術

３．求められる安全管理措置

（１）現行ガイドライン等での安全管理措置の規定の概要

法第 20 条では、個人情報取扱事業者に対し、取り扱う個人データの漏えい等が生じないよう安全管理措置を義務付けている。法第７条に基づき策定された「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定。以下「基本方針」という。）では、「事業運営において個人情報の保護を適切に位置づける観点から、外部からの不正アクセスの防御対策のほか、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、事業者の内部における責任体制を確保するための仕組みを整備することが重要である」として、安全管理措置の必要性を規定している。基本方針を踏まえ、監督官庁で定めるガイドラインで、個人情報の安全管理措置について具体的に規定している。

現行ガイドラインでは、「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」としている。現行ガイドラインの解説では、安全管理措置を大きく組織的保護措置と技術的保護措置の２つに分類し、その双方を適切に実行することが必要であるとしている。その中で、個人情報の社外への持出しについては、「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で規定した上で行うこと等）」と規定している。

（２）諸外国等での状況

①　諸外国での状況

諸外国では、多くの国で個人情報の保護に関する法令において個人情報の安全管理についての規定がなされているものの、持出時の安全管理措置について明確な規定を設けているものは多くない。

イギリス及びオーストラリアでは、監督機関の定めたガイドラインで、社外に持ち出す情報には暗号化措置を講じるという持出時の安全管理措置に言及している。カナダでは、「個人情報保護法　自己評価ツール」で、企業に対してテレワーク等個人情報の持出しを想定した社内規則を作成するよう求めている。また、韓国では、持出時の安全管理措置について明確な規定を設けてはいないものの、情報通信網を通じて利用者の個人情報を送受信する場合には、暗号化して送受信することを規定している。

一方、ドイツ、フランス、アメリカにおいては、持出時の安全管理措置について、ガイドライン等の指針を含め、明確な規定は設けられていない。

表５　諸外国における個人情報の安全管理措置

	主な個人情報保護制度	安全管理措置及び持出時の安全管理措置に関する規定について
イギリス	● 「1998年データ保護法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、ガイドラインに規定
フランス	● 「情報処理、情報ファイル及び自由に関する1978年1月6日の法律78-17号」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関しても、法律でカバーしているとの見解
ドイツ	● 「連邦データ保護法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
EU	● 「個人情報の取扱いに係る個人の保護及び当該情報の自由な移動に関する欧州議会及び理事の指令（データ保護指令）」を制定	● 安全管理措置については指令で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
韓国	● 「情報通信網利用促進及び情報保護に関する法律」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
オーストラリア	● 「1998年連邦プライバシー法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、インフォメーションシートに規定
カナダ	● 「連邦個人情報保護・電子文書法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、「個人情報保護法 自己評価ツール」により企業内で定めることを推奨
アメリカ	● 連邦法では、個別法にて個人情報保護を規定 ● 州法においては、個人情報保護法を制定	● 安全管理措置について個別の法律内で規定 ● 民間部門においては、持出時の安全管理措置に関する明確な規定は存在しない
（参考） 日本	● 個人情報の保護に関する法律を規定	● 安全管理措置については法律で規定 ● 持出時に関する規定は、各分野のガイドライン内において個別に規定

2009年　11月の状況

②　他分野のガイドラインでの状況

他分野のガイドラインでは、現在、持出時の安全管理措置について明確に規定しているものは少ない。そのような規定があるものとしては、金融分野のガイドライン

（「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」）及び医療・介護分野のガイドライン（「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」）が挙げられる。

金融分野のガイドラインでは、持ち出す個人データを必要最小限に限定する等の事項を盛り込んだ安全管理措置に関する規程を設けるよう規定している。医療・介護分野のガイドラインでは、持出しに関する方針や情報の管理方法を運用管理規程で定めること、情報機器に対して起動パスワード、情報に対して暗号化・アクセスパスワードを設定すること等を掲げており、人的・組織的安全対策の面に加えて、技術的安全対策の面からも対策を講じるよう規定している。

③　その他

個人情報保護のみを念頭に置いたものではないものの、安全・安心にテレワークを導入するための情報セキュリティ対策という観点から、総務省では、平成 16 年 12 月に、「テレワークセキュリティガイドライン」を作成している。平成 18 年４月の改訂の際には、同ガイドラインを援用しつつ、職場外でパソコンを使用する際に想定される様々な危険性を前提に、モデルケースとしての対策を例示した「職場外のパソコンで仕事をする際のセキュリティガイドライン」も作成している。同ガイドラインでは、必要な対策について、「ルール」についての対策、「人」についての対策、「技術」についての対策に分け、19 項目を規定している。

表６　テレワークセキュリティ対策１９か条

（「ルール」についての対策）
①管理規程（管理者の選任、情報資産の管理方法の策定等）を構築する。
②職場外でパソコンが使用される場合でも、管理規定が正しく守られているか、定期的なチェック（監査）を実施する。
③社内システムへアクセスするためのアカウントについては、管理方法を明確に定め、厳格に管理する。
④従業員にパソコンを貸し出す際には、「氏名」、「担当業務」、「パソコン機種」、「連絡先」、「返却期限」、「情報セキュリティ対策状況」 等を把握しておく。
⑤業務用に貸し出されたパソコンは許可された目的内で利用条件に従って適切に用いる。
⑥時的に職場外に持ち出す情報は原本ではなく、原本からの複製とする。
⑦私物のパソコンを業務に利用する場合には、インストールされているソフトを確認する等定められた利用条件に従う。
⑧ネットワークを用いて業務を実施する際には、指定された通信手段を用いる。

（「人」についての対策）
⑨トップダウンにより管理規程を周知・徹底する。
⑩従業員の情報セキュリティに関する認識を確実なものにするために、日々、教育・啓発活動を実施する。
⑪就業規則や外部委託契約に情報の持ち出しに当たっての許可等機密保持規定や罰則規定を設ける。
⑫漏えい事故発生時は、直ちに定められた担当者に連絡する。

（「技術」についての対策）
⑬ウイルス対策ソフトをインストールし、最新の定義ファイルに定期的に更新する。
⑭ＯＳ及びソフトウェアにおいては、パッチの更新を定期的に行う。
⑮ＯＳのログイン時等のパスワードは、他人に推測されにくいものとし、定期的に更新を行う。
⑯機密性の高い情報を持出・保存・送信する際には必ず暗号化する。
⑰社内システムと持ち出し用パソコンの環境の境界線にはファイアウォールやルータ等を設置し、不必要なアクセスを遮断する。
⑱社内システム内にある重要情報は、安全な領域に格納するとともにアクセス権限の付与は必要最低限とする。

※「職場外のパソコンで仕事をする際のセキュリティガイドライン（平成18年4月 総務省） 概要より抜粋

（３）持出時の安全管理措置を講じる際の考え方

モバイル PC 等による社外への個人情報の持出時に、個人情報の漏えいリスクに対応するために必要な安全管理措置を講じる場合には、リスクの評価、リスクに対応する措置の検討・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。

① リスクの評価

まず、持ち出す情報の種類、内容やその分量、持ち出す従業員の範囲や持ち出す方法、社内での管理状況等の関連する状況を踏まえ、どのようなリスクがどこで生じるのか等、個人情報の持出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。

② リスクに対応する措置の検討・決定

リスクの評価の後、それらのリスクに対応するために必要とされる安全管理措置を検討し、決定することが必要である。その際には、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となる。

まず、個々の技術的保護措置には、その技術の特性から強い点・弱い点が存在することから、それぞれの特性を把握した上で、リスクに適切に対応できるように具体的な措置を選択することが必要である。その際には、一つの措置で全てのリスクに対処するのではなく、複数の措置を適切に組み合わせることが重要である。

次に、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が必要である。導入コストをかけて部分的にセキュリティ強度を強固にしても、相対的に技術的に弱い部分があれば、その部分から問題が生ずるおそれがあるため、技術的に最も弱い部分を把握し、その部分に対応する措置が十分なものなのかを検討することが必要である。

さらに、技術的保護措置の検討に当たっては、措置を講ずることによる利便性への影響及び導入コストと、持ち出された個人情報の安全性の双方を勘案することが重要である。一般に、利便性や導入コストと安全性とはトレードオフの関係にあるため、評価したリスクについて、利便性や導入コストと安全性の双方のバランスを判断して適切な措置を決定することが必要である。

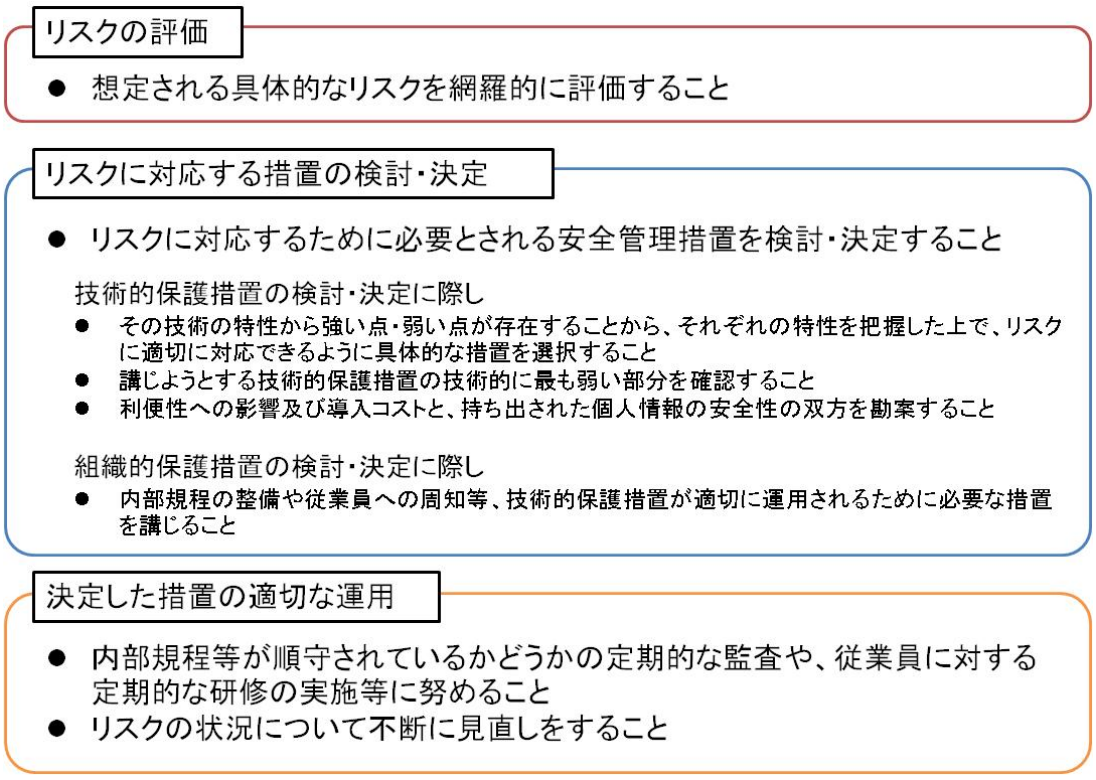
組織的保護措置については、内部規程の整備や従業員への周知等、技術的保護措置が適切に運用されるために必要な措置を講じることが必要である。

③ 決定した措置の適切な運用

リスクに対応する安全管理措置を決定しても、それが適切に運用されていないとリスクは低減されない。このため、内部規程等が順守されているかどうかの定期的な監査や、従業員に対する定期的な研修の実施等に努めることが必要である。さらに、持

出しの状況の変化や技術の進歩等、リスクの状況は変化していくものであるため、リスクの状況について不断に見直しをすることが必要である。

図 11　持出時の安全管理措置を講じる際の考え方



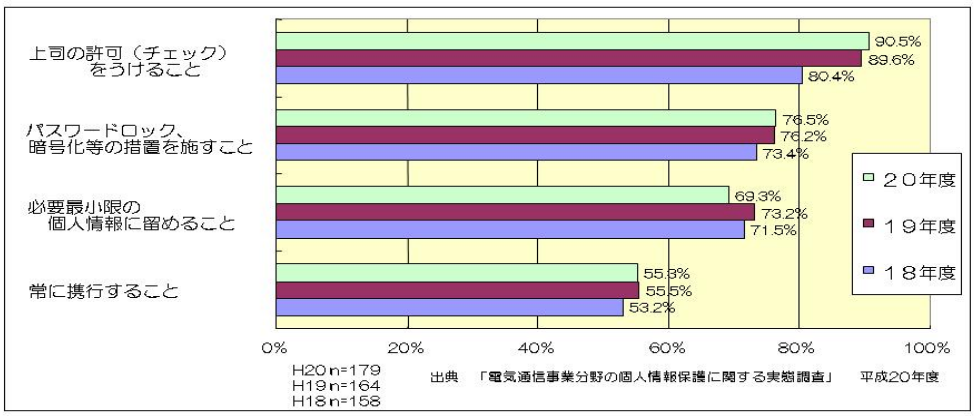
（４）技術的保護措置についての検討の必要性

安全管理措置は、前述のとおり、組織的保護措置と技術的保護措置の２つに大きく分けられる。モバイル PC 等による個人情報の社外への持出しに当たっての安全管理措置としては、その双方を一体的・総合的に講じることが必要である。

組織的保護措置については、内部規程の策定、適切な運用がなされているのかの監査、従業員の教育や監督等であり、講じるべき措置については、社内での個人情報の取扱いに関する措置と大きな相違点は存在しないものと思われる。ただし、具体的内容については、持出時にも対応するような内部規程の修正、持出時を対象とした監査、従業員の教育や監督等が必要になる。

一方で、技術的保護措置については、持出時の漏えいリスクに対応した技術的対応策がでてきており、それらは社内で用いられる技術的対応策とは異なるものも多く、具体的な留意点等も異なるものと思われる。また、現状としても、事業者によっては必ずしも適切な技術的保護措置が講じられていないものと思われる。前述の「平成 20 年度電気通信事業分野の個人情報保護に関する実態調査」では、社外に持ち出した業務用 PC で取り扱う個人情報に暗号化、パスワード設定等をしていると回答した事業者は 70%を超えており、ある程度の技術的保護措置が講じられている。しかし、法施行以来、電気通信事業分野における個人情報の漏えい事案として総務省に報告されたもののうち、ノート PC の紛失は 17 件あり、それらの事案で講じられていた技術的保護措置として、IC カードによる PC の起動制御に加え記録媒体の暗号化措置など、個人認証と暗号化による複数の安全管理措置を講じているケースが４件、暗号化措置のみを講じていたケースが１件、BIOS や OS へのパスワード措置を講じていたケースが 11 件、まったく措置をしていないものが１件で、必ずしも十分な安全管理措置が講じられているとはいえない状況である。

図 12　個人情報の入ったノート PC 等を社外に持ち出す場合のルール



このため、以下では、モバイル PC 等による個人情報の社外への持出しに当たって必要とされる安全管理措置について、技術的保護措置を中心に検討する。

（５）技術的保護措置を講じる場合の考え方

① 基本的事項

モバイル PC 等により個人情報を社外に持ち出す場合に必要とされる技術的保護措置に関する基本的事項として、次の事項が挙げられる。

ア モバイル PC 等を社外に持ち出す場合に必要な技術的保護措置

モバイル PC 等を社外に持ち出す場合には、常に紛失、盗難に遭うリスクがあり、その場合には、当該モバイル PC 等を権限のない者に使用されることによる漏えいリスクが生ずる。

このため、権限のない者に使用させないように、モバイル PC の BIOS、OS の起動時等で個人認証技術を導入することが必要である。

また、本来想定していなかった使用方法による個人情報の漏えいを防ぐため、通信カードや USB 等不必要な外部媒体について、内部規程で使用しないように定めるのみならず、物理的に接続を制限することが必要である。

さらに、持出先で通信カードや USB 等の外部媒体を接続する場合や、インターネットに接続する場合には、それらを通じてウイルスの侵入を受け、内部の情報が漏えいするおそれがある。そのような事態に備え、常にモバイル PC の OS・アプリケーションを最新のセキュリティ水準に維持するようにしておくことが必要である。

イ モバイル PC 等に情報を保存する場合に必要な技術的保護措置

モバイル PC 等に個人情報を含む情報を保存して社外に持ち出す場合には、紛失、盗難に遭った場合に、当該モバイル PC 等を権限のない者に使用されることによる漏えいリスクに加えて、記録媒体を物理的に取り出されることによる漏えいリスクも生ずる。

このため、持ち出す情報を暗号化することが必要である。その際、社外において個人情報を含む情報を保存することが考えられる場合には、保存した情報が常に暗号化されているようにし、暗号化されていない情報が持ち出したモバイル PC 等の内部に存在しないようにすることが必要である。

ウ モバイル PC をネットワークに接続する場合に必要な技術的保護措置

モバイル PC を用いて社外からネットワークに接続し、個人情報をやり取りする場合には、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクが生ずる。

このため、第三者から通信内容を盗み見られないよう、暗号化通信を行うか、やり取りするファイル自体を適切に暗号化することが必要である。

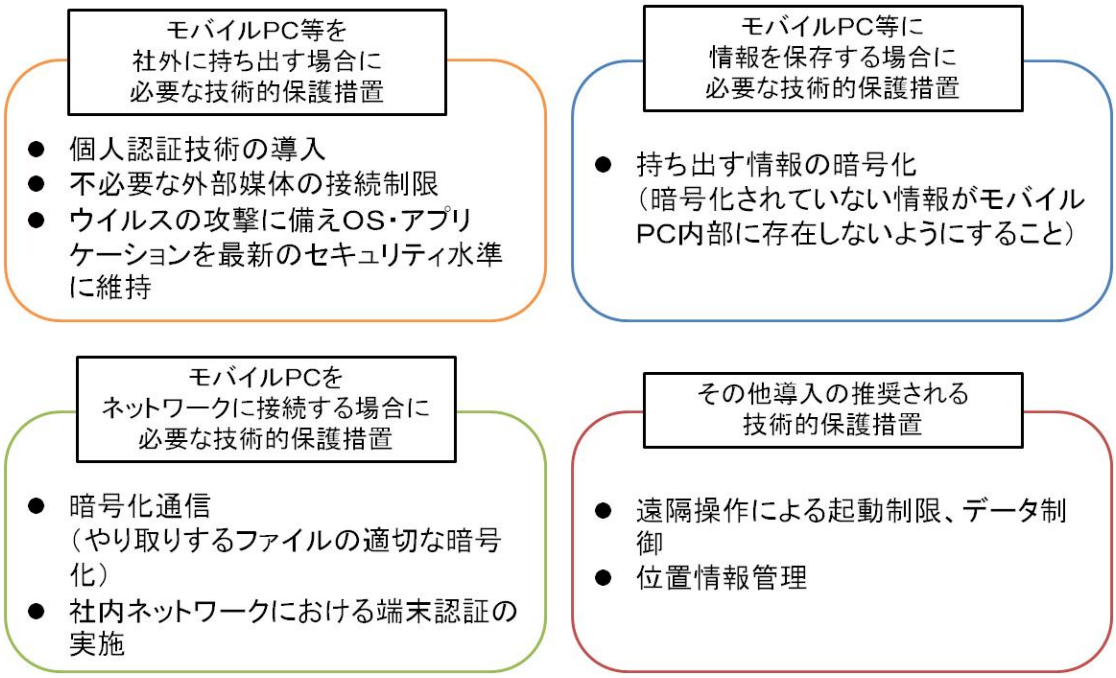
また、持ち出したモバイル PC から社内ネットワークに接続可能である場合には、第三者に社内ネットワークに侵入され、情報を盗み見られるおそれもある。

そのような事態を防ぐために、社内サーバ側においてクライアント認証を実施し、社内ネットワークに入る権限のある者だけが情報を見ることができるように措置を講じることが必要である。

エ　その他の措置

現在、モバイル PC の紛失、盗難に備え、遠隔操作によって起動制限、データ制御、位置情報管理等を行う技術も存在する。これらについては、導入することによりさらに個人情報の漏えいリスクに対応することが可能になるため、以上のような措置に加えて導入しておくことが推奨される。

図 13　利用状況に応じて必要とされる、持出時の技術的保護措置



② 個別技術に関する留意事項

それぞれの技術的保護措置を講じる場合には、適切な安全性を確保するために、その技術に応じ、以下のような点に留意する必要がある。

ア 個人認証技術

個人認証技術を講じるに当たっては、本人認証性を高め、第三者が簡単に個人認証を破ってモバイル PC 等を使用することがないよう、それぞれの認証技術に応じ、以下の点に留意することが必要である。また、複数の認証技術を組み合わせ、二重三重の認証を講じることが望ましい。

（ア）パスワード等記憶による認証

認証に用いるパスワードは、第三者から容易に推測されないよう、辞書等に記載されている単語を避けること、複数の英数特殊文字を組み合わせること、適切な文字数以上の長さのものを使用すること等に注意することが必要である。また、定期的にパスワードを変更することが必要であり、その際には、少数のパスワードを定期的に使いまわすことは避けるべきである。これらの条件を満たしたパスワードを自動生成ソフトによって作成することや、また、システム的に不適切なパスワードは設定できないようにすることが可能な場合もある。

また、従業員によるパスワードの管理が適切に行われることも必要である。具体的には、メモ等に書き込んで放置したりしないこと、ソフトウェアに記憶させないこと等他人に知られないようにすることが必要である。

コンピュータを用いた総当たり攻撃によって権限のない第三者が認証を破ることも考えられるため、認証に複数回失敗した場合には、一定時間認証を不可能にすることや、その後の認証自体を不可能にする等の措置を講じることが望ましい。

（イ）IC カード等所有物による認証

所有物とモバイル PC を同時に紛失、盗難に遭った場合には、容易に認証を破られてしまうことから、同時に紛失、盗難に遭わないように適切に管理することが必要である。また、それに加えて、所有物による認証時に、パスワードによる認証も併せて実施することが望ましい。

（ウ）指紋等生体情報による認証

生体情報による認証の中でも、音声認証や顔認証のように他人受入率が１％～0.1%のものもあれば、指紋認証や静脈認証のように他人受入率が 0.001%～0.00001%のものもあるなど、その方式により本人認証性に差がある点に注意して、導入する方法を選択することが必要である。

イ　暗号化措置・鍵の管理

（ア）暗号アルゴリズム

暗号化措置を講じるに当たっては、技術的な確証がある暗号アルゴリズムを用いることが必要である。具体的には、公的機関による客観的評価がなされているものとして、CRYPTREC で策定された電子政府推奨暗号リストや ISO/IEC で策定された国際標準規格 ISO/IEC18033 で公表されている暗号アルゴリズムを使用することが強く推奨される。

（イ）復号鍵の管理

情報を暗号化していたとしても、復号鍵が第三者に利用されては、暗号化は意味をなさない。そのため第三者が容易に復号鍵を入手できないように、復号鍵の管理を適切に行うことが必要である。

最も確実な方法として、復号鍵を暗号化された情報から物理的に分けて管理する方法がある。例えば、IC カード等の別の媒体の中に復号鍵を保管する方法や秘密分散法により復号鍵を分散する方法がある。この場合には、その媒体がモバイル PC と同時に紛失、盗難に遭うことがないよう管理を徹底すること、媒体による復号時にパスワードによる認証を併せて実施すること等の措置を講じることが望ましい。

復号鍵をモバイル PC と物理的に分けて管理しない場合には、常にモバイル PC と同時に紛失、盗難に遭うリスクが存在する。その場合には、復号鍵を盗みだそうとする攻撃から守ることのできる耐タンパ性を持った、モバイル PC 中のチップ上で管理する方法が考えられる。また、紛失、盗難に遭った際に、復号鍵を遠隔操作により削除し、第三者が復号鍵を入手できないようにすることも考えられる。

（ウ）暗号化の対象

暗号化の対象としては、個別のファイル、特定のフォルダ、記録媒体全体等の中から選択することになる。

ファイル、フォルダの暗号化の場合には、暗号化の対象外となる情報があるため、個人情報を含む情報が確実に暗号化されるようにすることが必要である。特に、自動的に生成される作業用ファイルやバックアップファイル等については、ソフトウェアによって格納される場所が異なることから、注意が必要である。

ウ　遠隔データ管理技術

遠隔操作によりモバイル PC を管理する場合には、通信可能な圏外に持ち出された場合等、遠隔操作が不可能となる事態や指示を実行するまでにモバイル PC を使用さ

れる事態をあらかじめ想定し、個人認証技術や情報の暗号化等の他の技術と組み合わせて対応することが必要である。

　また、遠隔操作の指示をしたとしても、それが正しく実行されない可能性もあるため、指示の実行状況を把握できるようにすることが望ましい。

（６）導入コスト等

以上で見てきた技術的保護措置については、現在、それほど多額の費用をかけることなく、最低限の安全性が確保できる措置の導入が可能である。

例えば、暗号化措置については、OS に標準装備されている機能や、一般に市販されているソフトウェアによって導入することが可能である。個人認証についても、パスワード認証は、モバイル PC の BIOS や多くの OS やソフトウェアで設定が可能である。また、多くのモバイル PC では USB ポートを標準装備しており、USB キーを利用した所有物による認証の導入のコストは大きくない。さらに、指紋認証のための読取機能があらかじめ内蔵されている PC も存在する。

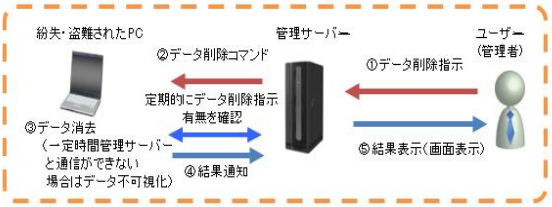
携帯電話端末については、現在、それぞれの事業者により具体的な機能は異なるが、紛失、盗難時に備え、端末のロック機能や指紋認証等、携帯電話端末に保存された情報を保護するための機能が提供されている。

さらに、様々な機能を組み合わせて、一定レベルの安全性を確保するサービスも存在している。それぞれのサービスにより対応するリスクや確保される安全性の程度が異なり、また、導入に係る費用も異なっている。このため、そのようなサービスを利用する場合には、どのような技術が組み合わされており、どのようなリスクに対して、どれだけの安全性が確保されているのか等を確認し、自社におけるリスクへの対応として十分であるのかを検討することが必要である。

図 14　現在あるソリューション事例

【ソリューション事例】（KDDI株式会社）　平成21年11月時点

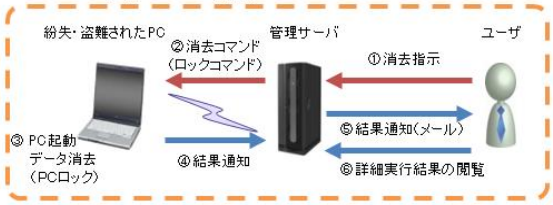
遠隔操作によって該当データの上書きを指示し、データを削除



- 遠隔操作でPCの指定されたデータを削除（データの上書き）
- インターネット接続中は、定期的に管理サーバーと通信し、データ削除指示有無を確認
  インターネット接続がない環境でも、PCにKDDI指定の通信カード等を使用の場合、電源ON時等に強制的に管理サーバーと通信し、データ削除指示有無を確認
- 一定時間管理サーバと通信ができない場合は、指定されたデータを不可視化

【ソリューション事例】（富士通株式会社、株式会社ウィルコム）

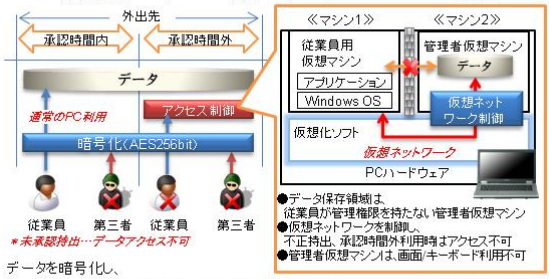
遠隔操作によって、PCの起動制限、データの復号鍵を消去し、ハードディスク内データを消去



- 遠隔操作でPCの起動を制限（PCロック）
- 遠隔操作でPCのハードディスク内の全データを即時消去（復号鍵の消去）
- PCが電源オフ状態でも実行可能（専用の通信モジュールを搭載）
- 消去結果や、PCへのアクセス履歴を含むレポートを通知

【ソリューション事例】（株式会社 東芝）

データ保存領域のアクセスを制御し外出時のセキュリティを強化

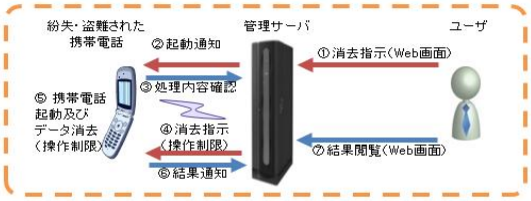


データを暗号化し、

- 承認時間内は、パスワード等がないと利用不可（パスワード等を持ち得ない第三者は、利用不可）
- 承認時間外は、パスワード等があっても利用不可（従業員であっても、利用不可）

【ソリューション事例】（株式会社NTTドコモ）

遠隔操作によって操作制限や、データ消去プログラムを起動し、携帯電話内のデータを消去



- 遠隔操作で端末の操作を制限
- 遠隔操作で携帯電話の全データを消去し、工場出荷時に戻す
- 本体のみならず、SIMカード内の電話帳データやmicroSD内も削除
- 消去指示結果を通知（５分程度で操作履歴画面に反映）

（７）個人情報の持出しに関する留意点

モバイル PC 等による個人情報の社外への持出しに際して、適切な技術的保護措置を講じることにより、モバイル PC 等が紛失、盗難に遭っても、被害を最小限に抑えることが可能な場合もある。

しかし、技術的保護措置を講じているからといって、紛失、盗難に遭っても良いものではなく、そのような事態にならないように、モバイル PC 等が適切に管理されるようにすることが必要である。

また、持ち出す個人情報は、業務上必要最小限の範囲にすることが必要である。例えば、業務上必要な分量を超えた個人情報や業務上必要でない種類の個人情報を持ち出すことは避けるべきである。その際、現行ガイドライン第４条で取得を制限しているいわゆるセンシティブ情報等、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すことのないようにするとともに、持ち出す必要がある場合には、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じることが必要である。