# 情報サービス産業　個人情報保護ガイドライン

# （第４版）　目次

# 情報サービス産業　個人情報保護ガイドライン

# （第４版）

一般社団法人情報サービス産業協会

## 序　文

当協会は、わが国における情報サービス産業を代表する団体として情報化の進展と個人情報保護の重要性を認識し、情報サービス事業者の個人情報保護への自主的な取組みを促進・支援するため、平成元年に「情報サービス産業　個人情報保護ガイドライン」を策定以来、国内外の情勢の変化に対応し平成９年、平成12年に改定を行うなど、産業界をリードしてその普及・啓発を図るとともに、個人情報保護の強化に取り組んできた。

また、平成10年４月に創設された「プライバシーマーク制度」における第１号の付与認定指定機関として圧倒的な認定企業数を誇るなど、プライバシーマーク制度の普及にも努めてきた。

この度、個人情報の適切な保護について、事業者が体系的で経営活動全般を統合した個人情報保護マネジメントシステムを確立するための規範として日本工業規格「個人情報保護マネジメントシステム －要求事項」（JIS Q 15001:2006）が改定されたことにともない、社団法人情報サービス産業協会では、今回業界ガイドラインをこれに準拠して見直し、大幅に改定した。

情報サービス事業者は、個人情報を含む多種多様な情報を大量に取り扱う者の当然の責務として個人情報の適切な保護に努めなければならないが、そのためには、このガイドラインに準拠した個人情報保護マネジメントシステムを確立し、実施し、維持し、継続的に改善していくことが必要である。なお、情報サービス事業者は、個人情報保護マネジメントシステムを策定するに当って、それぞれの事業活動の実態に照らし個人情報との係わりを的確に把握した上で、このガイドラインに規定した事項のほかに必要な項目を追加することが望まれる。また、委託先企業にも同様の対応をとるよう要請することも、個人情報保護を担保する上で実務上有用であろう。

このガイドラインは、情報サービス事業者のコンプライアンス経営の推進の一翼を担うものであり、自由かつ公正な競争を阻害するものではない。

情報サービス事業者は、自由な情報流通の確保を前提としたユビキタス社会の進展に貢献し、個人情報の保護の必要性と個人情報の利用の有用性を共に認識し、両者を調和させるよう努めるものである。

## 第１章　総　則

**（適用範囲）**

**第1条**　このガイドラインは、個人情報を事業の用に供している、あらゆる種類、規模の情報サービス事業者に適用できる個人情報保護マネジメントシステムに関する要求事項について規定する。

**2.**　情報サービス事業者は、次の事項を行う際に、このガイドラインを用いることができる。

(1) 個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善すること

(2) 策定した個人情報保護マネジメントシステムがこのガイドラインに適合していることについて自ら確認し、適合していることを自ら表明すること

(3) 策定した個人情報保護マネジメントシステムがこのガイドラインに適合していることについて組織外部又は本人に確認を求めること

(4) 組織外部による個人情報保護マネジメントシステムの認証又は登録を求めること

**（定義）**

**第2条**　このガイドラインで用いる用語の定義は、次による。

(1) **個人情報**　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などによって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、それによって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。

(2) **本人**　個人情報によって識別される特定の個人をいう。

(3) **情報サービス事業者**　情報サービス業を営む事業者（法人、その他団体又は個人）をいう。

(4) **従業者**　情報サービス事業者の組織内にあって、直接又は間接に情報サービス事業者の指揮監督を受けて当該情報サービス事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員など）のみならず、取締役、執行役、理事、監査役、監事、派遣社員も含まれる。

(5) **個人情報保護管理者**　代表者によって情報サービス事業者の内部の者から指名された者であって、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を有する者をいう。なお、個人情報保護管理者は、やむを得ない場合を除いて、当該情報サービス事業者の内部に権限、影響力を有する役員レベルを任命すべきものとする。

(6) **個人情報保護監査責任者**　代表者によって情報サービス事業者の内部の者から指名された者であって、個人情報保護管理者から独立した公平、かつ、客観的な立場にあり、監査の実施及び報告を行う責任及び権限を有する者をいう。

(7) **個人情報保護教育責任者**　代表者又は個人情報保護管理者によって情報サービス事業者の内部の者から指名された者であって、個人情報保護管理者を補佐して、従業者及び取扱いの委託先の教育の実施並びに報告を行う責任及び権限を有する者をいう。

(8) **本人の同意**　本人が、個人情報の取扱いに関する情報を与えられた上で、自己に関する個人情報の取扱いについて承諾する意思表示をいう。ただし、本人が子ども又は事理を弁識する能力を欠く者の場合は、法定代理人などの同意も得なければならない。

(9) **個人情報保護マネジメントシステム**　情報サービス事業者が、自らの事業の用に供する個人情報について、その有用性を配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、運用の確認及び見直しを含むマネジメントシステムをいう。

(10) **不適合**　このガイドラインに規定する要求を満たしていないことをいう。

**（一般要求事項）**

**第3条**　情報サービス事業者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善しなければならない。

**（個人情報保護方針）**

**第4条**　情報サービス事業者の代表者は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない。

(1) 情報サービス事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、「目的外利用」という。）を行わないこと及びそのための措置を講じることを含む。）

(2) 個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守すること

(3) 個人情報の漏えい、滅失又はき損の防止及び是正に関すること

(4) 苦情及び相談への対応に関すること

(5) 個人情報保護マネジメントシステムの継続的改善に関すること

(6) 代表者の氏名

**2.**　情報サービス事業者の代表者は、この方針を文書（電子的方式、磁気的方式その他人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）化し、従業者に周知させるとともに、一般の人が入手可能な措置を講じなければならない。

## 第2章　体制及び責任

**（資源、役割、責任及び権限）**

**第5条**　情報サービス事業者の代表者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善するために不可欠な資源を用意しなければならない。

**2.**　情報サービス事業者の代表者は、個人情報保護マネジメントシステムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、従業者に周知しなければならない。

**（個人情報保護管理者、監査責任者、教育責任者及び対応窓口の指名）**

**第6条**　情報サービス事業者の代表者は、このガイドラインの内容を理解し実践する能力のある個人情報保護管理者を当該事業者の内部の者から指名し、個人情報保護マネジメントシステムの実施並びに運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。

**2.**　個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、情報サービス事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない。

**3.**　情報サービス事業者の代表者は、このガイドラインの内容を理解し、個人情報保護に関する監査を行う能力のある個人情報保護監査責任者を当該事業者の内部の者から指名し、個人情報保護マネジメントシステムの監査に関する責任及び権限を与え、監査を行わせなければならない。

**4.**　情報サービス事業者の代表者は、このガイドラインの内容を理解し、個人情報保護に関する適切な教育を行う能力のある個人情報保護教育責任者を当該事業者の内部の者から指名し、個人情報保護マネジメントシステムの教育に関する責任及び権限を与え、従業者

及び委託先の教育を行わせなければならない。なお、個人情報保護管理者が自ら行っても良い。

**5.** 個人情報保護管理者は、個人情報の取扱い及び個人情報保護マネジメントシステムに関しての本人からの苦情及び相談を受け付けて対応する窓口を常設し、当該窓口の連絡先を本人に告知しなければならない。

## 第3章　計　画

**（個人情報の特定）**

**第7条**　情報サービス事業者は、自らの事業の用に供するすべての個人情報を特定するための手順を確立し、かつ、維持しなければならない。

**（法令及びその他の規範）**

**第8条**　情報サービス事業者は、個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し、参照できる手順を確立し、かつ、維持しなければならない。

**（リスク等の認識・分析及び対策）**

**第9条**　情報サービス事業者は、特定した個人情報について、目的外利用を行わないために必要な対策を講じる手順を確立し、維持しなければならない。

**2.** 情報サービス事業者は、特定した個人情報について、その取扱いの各局面におけるリスク（個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ）を認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

**（内部規程）**

**第10条**　情報サービス事業者は、個人情報に関わる次の事項を含む内部規程を文書化し、かつ、維持しなければならない。

(1) 個人情報を特定する手順に関する規定
(2) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定
(3) 個人情報に関するリスクの認識、分析及び対策の手順に関する規定
(4) 情報サービス事業者の各部門及び階層における個人情報を保護するための権限及び責任に関する規定
(5) 緊急事態（個人情報が漏えい，滅失又はき損をした場合）への準備及び対応に関する規定
(6) 個人情報の取得、利用及び提供に関する規定
(7) 個人情報の適正管理に関する規定
(8) 本人からの開示等の求めへの対応に関する規定
(9) 教育に関する規定
(10) 個人情報保護マネジメントシステム文書の作成及び管理に関する規定
(11) 苦情及び相談への対応に関する規定
(12) 運用の確認に関する規定
(13) 監査に関する規定
(14) 是正処置及び予防処置に関する規定

(15) 代表者による個人情報保護マネジメントシステムの見直しに関する規定
(16) 内部規程の違反に関する罰則の規定

**2.** 情報サービス事業者は、事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように内部規程を改定しなければならない。

**（計画書）**

**第11条** 情報サービス事業者は、個人情報保護マネジメントシステムを確実に実施するために必要な教育、監査などの計画を少なくとも年1回以上立案し、文書化し、かつ、維持しなければならない。

**（緊急事態への準備）**

**第12条** 情報サービス事業者は、緊急事態を特定するための手順、また、それらにどのように対応するかの手順を確立し、実施し、かつ、維持しなければならない。

**2.** 情報サービス事業者は、個人情報が漏えい、滅失又はき損をした場合に想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とするための手順を確立し、かつ、維持しなければならない。

**3.** 情報サービス事業者は、個人情報の漏えい、滅失又はき損が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持しなければならない。

(1) 当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くこと
(2) 二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること
(3) 事実関係、発生原因及び対応策を関係機関に直ちに報告すること
(4) 顧客から取扱いの委託を受けた個人情報の漏えい、滅失又はき損に関して、直ちに委託元に報告すること

## 第4章 実施及び運用

### 第１節 運用手順

**（運用手順）**

**第13条** 情報サービス事業者は、個人情報保護マネジメントシステムを確実に実施するために、運用の手順を明確にしなければならない。

### 第2節 個人情報の取得・利用及び提供に関する原則

**（利用目的の特定）**

**第14条** 情報サービス事業者は、個人情報を取得するに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない。

**（適正な取得）**

**第15条** 情報サービス事業者は、適法、かつ、公正な手段によって個人情報を取得しなければならない。

**（特定の機微な個人情報の取得・利用及び提供の制限）**

**第16条**　情報サービス事業者は、次に示す内容を含む個人情報の取得、利用又は提供を行ってはならない。ただし、これらの取得、利用又は提供について、明示的な本人の同意がある場合、及び第19条のただし書き(1)～(4)のいずれかに該当する場合は、この限りでない。

(1) 思想、信条又は宗教に関する事項
(2) 人種、民族、門地、本籍地（所在都道府県に関する情報を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項
(3) 勤労者の団結権、団体交渉その他団体行動の行為に関する事項
(4) 集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項
(5) 保健医療又は性生活に関する事項

**（本人から直接書面によって取得する場合の措置）**

**第17条**　情報サービス事業者は、本人から、書面（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ）に記載された個人情報を直接に取得する場合には、少なくとも、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、書面によって本人に明示し、本人の同意を得なければならない。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、第18条のただし書き(1)～(4)及び第19条のただし書き(1)～(4)のいずれかに該当する場合は、この限りでない。

(1) 情報サービス事業者の名称
(2) 個人情報保護管理者又はその代理人の氏名又は職名、所属及び連絡先
(3) 利用目的
(4) 個人情報を第三者に提供することが予定される場合には次の各事項
    ① 第三者に提供する目的
    ② 提供する個人情報の項目
    ③ 提供の手段又は方法
    ④ 当該情報の提供を受ける者又は提供を受ける者の組織の種類及び属性
    ⑤ 個人情報の取扱いに関する契約がある場合はその旨
(5) 個人情報の取扱いの委託を行うことが予定される場合にはその旨
(6) 第29条～第32条に該当する場合には、その求めに応じる旨及び問い合わせ窓口
(7) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果
(8) 本人が容易に認識できない方法によって個人情報を取得する場合にはその旨

**（個人情報を直接書面以外の方法によって取得した場合の措置）**

**第18条**　情報サービス事業者は、個人情報を第17条以外の方法によって取得した場合は、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。ただし、次に示すいずれかに該当する場合は、この限りではない。

(1) 利用目的を本人に通知し、又は公表することによって本人若しくは第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
(2) 利用目的を本人に通知し、又は公表することによって当該情報サービス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
(3) 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って当該事務

の遂行に支障を及ぼすおそれがあるとき
(4) 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

## 第3節　個人情報の利用及び提供に関する措置

**（利用に関する措置）**

**第19条**　情報サービス事業者は、特定した利用目的の達成に必要な範囲内で個人情報を利用しなければならない。特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合は、あらかじめ、少なくとも、第17条(1)～(6)に示す事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りではない。

(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、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、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って当該事務の遂行に支障を及ぼすおそれがあるとき

**（本人にアクセスする場合の措置）**

**第20条**　情報サービス事業者は、個人情報を利用して本人にアクセスする場合には、本人に対して、第17条(1)～(6)に示す事項又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りではない。

(1) 第17条(1)～(6)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、既に本人の同意を得ているとき
(2) 個人情報の取扱いの全部又は一部を委託された場合であって、当該個人情報を、その利用目的の達成に必要な範囲内で取り扱うとき
(3) 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、個人情報を提供する事業者が、既に第17条(1)～(6)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき
(4) 個人情報が特定の者との間で共同して利用され、共同利用者が、既に第17条(1)～(6)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、次に示す事項又はそれと同等以上の内容の事項を、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
    ① 共同して利用すること
    ② 共同して利用される個人情報の項目
    ③ 共同して利用する者の範囲
    ④ 共同して利用する者の利用目的
    ⑤ 共同して利用する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
    ⑥ 取得方法
(5) 第18条のただし書き(4)に該当するため、利用目的などを本人に明示、通知又は公表することなく取得した個人情報を利用して、本人にアクセスするとき

(6) 第19条のただし書き(1)～(4)のいずれかに該当する場合

**（提供に関する措置）**

**第21条** 情報サービス事業者は、個人情報を第三者に提供する場合には、あらかじめ本人に対して、取得方法及び第17条(1)～(4)の事項又はそれと同等以上の内容の事項を通知し、本人の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りではない。

(1) 第17条又は第20条の規定によって、既に第17条(1)～(4)の事項又はそれと同等以上の内容の事項を本人に明示又は通知し、本人の同意を得ているとき

(2) 大量の個人情報を広く一般に提供するため、本人の同意を得ることが困難な場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ本人に通知し、又はそれに代わる同等の措置を講じているとき

① 第三者への提供を利用目的とすること

② 第三者に提供される個人情報の項目

③ 第三者への提供の手段又は方法

④ 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

⑤ 取得方法

(3) 法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって、かつ、法令に基づき又は本人若しくは当該法人その他の団体自らによって公開又は公表された情報を提供する場合であって、(2)で示す事項又はそれと同等以上の内容の事項を、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

(4) 特定した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とき

(5) 合併その他の事由による事業の承継に伴って個人情報を提供する場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき

(6) 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、次に示す事項又はそれと同等以上の内容の事項を、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

① 共同して利用すること

② 共同して利用される個人情報の項目

③ 共同して利用する者の範囲

④ 共同して利用する者の利用目的

⑤ 共同して利用する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

⑥ 取得方法

(7) 第19条のただし書き(1)～(4)のいずれかに該当する場合

## 第4節　個人情報の適正管理

**（個人情報の正確性の確保）**

**第22条** 情報サービス事業者は、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、最新の状態で管理しなければならない。

**（安全管理措置）**

**第23条**　情報サービス事業者は、個人情報のリスクに応じて、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を講じなければならない。

**（従業者の監督）**

**第24条**　情報サービス事業者は、その従業者に個人情報を取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、当該従業者に対し必要かつ適切な監督を行わなければならない。

**（委託先の監督）**

**第25条**　情報サービス事業者は、個人情報の取扱いの全部又は一部を委託する場合は、十分な個人情報の保護水準を満たしている者を選定しなければならない。このため、情報サービス事業者は、委託を受ける者を選定する基準を確立しなければならない。

**2.**　情報サービス事業者は、個人情報の取扱いの全部又は一部を委託する場合は、委託する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わなければならない。

**3.**　情報サービス事業者は、次に示す事項を契約によって規定し、十分な個人情報の保護水準を担保しなければならない。

(1) 委託者及び受託者の責任の明確化
(2) 個人情報の安全管理に関する事項
(3) 再委託に関する事項
(4) 個人情報の取扱い状況に関する委託者への報告の内容及び頻度
(5) 契約内容が遵守されていることを委託者が確認できる事項
(6) 契約内容が遵守されなかった場合の措置
(7) 事件・事故が発生した場合の報告・連絡に関する事項

**4.**　情報サービス事業者は、前項の当該契約書などの書面を、少なくとも個人情報の保有期間にわたって保存しなければならない。

## 第5節　開示対象個人情報に関する本人の権利

**（開示対象個人情報に関する権利）**

**第26条**　情報サービス事業者は、電子計算機を用いて検索することができるように体系的に構成した情報の集合物又は一定の規則に従って整理、分類し、目次、索引、符~~合~~号などを付すことによって特定の個人情報を容易に検索できるように体系的に構成した情報の集合物を構成する個人情報であって、情報サービス事業者が、本人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するもの（以下、「開示対象個人情報」という。）に関して、本人から利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止（以下、「開示等」という。）を求められた場合は、第29条から第32条の規定によって、遅滞なくこれに応じなければならない。ただし、次のいずれかに該当する場合は、開示対象個人情報ではない。

(1) 当該個人情報の存否が明らかになることによって、本人若しくは第三者の生命、身体若しくは財産に危害が及ぶおそれのあるもの
(2) 当該個人情報の存否が明らかになることによって、違法又は不当な行為を助長し、又は誘発するおそれのあるもの

(3) 当該個人情報の存否が明らかになることによって、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のあるもの
(4) 当該個人情報の存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序維持に支障が及ぶおそれのあるもの

**（開示対象個人情報の開示等の求めに応じる手続）**

**第27条**　情報サービス事業者は、開示対象個人情報の開示等の求めに応じる手続として、次の事項を定めなければならない。

(1) 開示等の求めの申し出先
(2) 開示等の求めに際して提出すべき書面の様式その他の開示等の求めの方式
(3) 開示等の求めをする者が、本人又は代理人であることの確認の方法
(4) 第29条又は第30条による場合の手数料を定めた場合はその徴収方法

**2.**　情報サービス事業者は、本人からの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しなければならない。

**3.**　情報サービス事業者は、第29条又は第30条によって本人からの求めに応じる場合に、手数料を徴収するときは、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、その額を定めなければならない。

**（開示対象個人情報に関する事項の周知など）**

**第28条**　情報サービス事業者は、取得した個人情報が開示対象個人情報に該当する場合は、当該開示対象個人情報に関し、次の事項を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。）に置かなければならない。

(1) 情報サービス事業者の名称
(2) 個人情報保護管理者又はその代理人の氏名又は職名、所属及び連絡先
(3) すべての開示対象個人情報の利用目的（ただし、第18条第1項(1)～(3)に該当する場合を除く。）
(4) 開示対象個人情報の取扱いに関する苦情の申し出先
(5) 当該情報サービス事業者が個人情報の保護に関する法律（平成15年法律第57号）第37条第1項の認定を受けた者（以下「認定個人情報保護団体」という。）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し出先
(6) 第27条によって定めた手続

**（開示対象個人情報の利用目的の通知）**

**第29条**　情報サービス事業者は、本人から、当該本人が識別される開示対象個人情報について、利用目的の通知を求められた場合には、遅滞なくこれに応じなければならない。ただし、第18条第1項(1)～(3)のいずれかに該当する場合又は第28条(3)によって当該本人が識別される開示対象個人情報の利用目的が明らかな場合は、利用目的の通知を必要としないが、そのときは本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。

**（開示対象個人情報の開示）**

**第30条**　情報サービス事業者は、本人から、当該本人が識別される開示対象個人情報の開示（当該本人が識別される開示対象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。）を求められたときは、法令の規定によって特別の手続が定められている場合を除き、

本人に対し、遅滞なく、当該開示対象個人情報を書面（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）によって開示しなければならない。ただし、開示することによって次の(1)～(3)のいずれかに該当する場合は、その全部又は一部を開示する必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。

(1) 本人若しくは第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
(2) 当該情報サービス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
(3) 法令に違反することとなる場合

**（開示対象個人情報の訂正、追加又は削除）**

**第31条** 情報サービス事業者は、本人から、当該本人が識別される開示対象個人情報の内容が事実でないという理由によって当該開示対象個人情報の訂正、追加又は削除（以下、本条において「訂正等」という。）を求められた場合は、法令の規定によって特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該開示対象個人情報の訂正等を行わなければならない。また、情報サービス事業者は、訂正等を行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正等を行わない旨の決定をしたときは、その旨及びその理由を、本人に対し、遅滞なく通知しなければならない。

**（開示対象個人情報の利用又は提供の拒否権）**

**第32条** 情報サービス事業者が、本人から当該本人が識別される開示対象個人情報の利用の停止、消去又は第三者への提供の停止（以下、本条において「利用停止等」という。）を求められた場合、これに応じなければならない。また、措置を講じた後は、遅滞なくその旨を本人に通知しなければならない。ただし、次の(1)～(3)のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。

(1) 本人若しくは第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
(2) 当該情報サービス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
(3) 法令に違反することとなる場合

## 第6節　教　育

**（教育）**

**第33条** 情報サービス事業者は、従業者に、少なくとも年1回以上適切な教育を行わなければならない。

**2.** 情報サービス事業者は、関連する各部門及び階層において、その従業者に次の事項を理解させる手順を確立し、かつ、維持しなければならない。

(1) 個人情報保護マネジメントシステムに適合することの重要性及び利点
(2) 個人情報保護マネジメントシステムに適合するための役割及び責任
(3) 個人情報保護マネジメントシステムに違反した際に予想される結果

**3.** 情報サービス事業者は、教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならない。

## 第7節　文書作成及び文書管理

**（文書の範囲）**

**第34条**　情報サービス事業者は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならない。

(1) 個人情報保護方針
(2) 内部規程
(3) 計画書
(4) このガイドラインが要求する記録及び情報サービス事業者が個人情報保護マネジメントシステムを実施する上で必要と判断した記録

**（文書の管理）**

**第35条**　情報サービス事業者は、このガイドラインが要求するすべての文書（記録を除く。）を管理する手順を確立し、実施し、かつ、維持しなければならない。

**2.**　文書管理の手順には、次の事項が含まれなければならない。

(1) 文書の発行及び改訂に関すること
(2) 文書の改訂の内容と版数との関連付けを明確にすること
(3) 必要な文書が必要なときに容易に参照できること

**（記録の管理）**

**第36条**　情報サービス事業者は、個人情報保護マネジメントシステム及びこのガイドラインの要求事項への適合を実証するために必要な記録を作成し、かつ、維持しなければならない。

**2.**　情報サービス事業者は、記録の管理についての手順を確立し、実施し、かつ、維持しなければならない。

## 第8節　苦情及び相談

**（苦情及び相談）**

**第37条**　情報サービス事業者は、個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切、かつ、迅速な対応を行う手順を確立し、かつ、維持しなければならない。

**2.**　情報サービス事業者は、上記の目的を達成するために必要な体制の整備を行わなければならない。

## 第9節　運用の確認

**（運用の確認）**

**第38条**　情報サービス事業者は、個人情報保護マネジメントシステムが適切に運用されていることを当該情報サービス事業者の各部門及び階層において定期的に確認するための手順を確立し、実施し、かつ、維持しなければならない。

## 第5章　監　査

**（監査）**

**第39条**　情報サービス事業者は、個人情報保護マネジメントシステムのこのガイドラインへの適合状況及び個人情報保護マネジメントシステムの運用状況を、少なくとも年1回以上監査しなければならない。

**2.**　情報サービス事業者の代表者は、公平、かつ、客観的な立場にある個人情報保護監査責任者を当該情報サービス事業者の内部の者から指名し、監査の実施並びに報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行なわせなければならない。

**3.**　個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、情報サービス事業者の代表者に報告しなければならない。なお、監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならない。

**4.**　情報サービス事業者は、監査の計画及び実施、結果の報告並びにこれに伴う記録の保持に関する責任と権限を定める手順を確立し、実施し、かつ、維持しなければならない。

**（是正処置及び予防処置）**

**第40条**　情報サービス事業者は、不適合に対する是正処置及び予防処置を確実に実施するための責任と権限を定める手順を確立し、実施し、かつ、維持しなければならない。その手順には、以下の事項を含めなければならない。

(1) 不適合の内容を確認すること
(2) 不適合の原因を特定し、是正処置及び予防処置を立案すること
(3) 期限を定め、立案された適切な処置を実施すること
(4) 実施された是正処置及び予防処置の結果を記録すること
(5) 実施された是正処置及び予防処置の有効性をレビューすること

## 第6章　個人情報保護マネジメントシステムの見直し

**（情報サービス事業者の代表者による見直し）**

**第41条**　情報サービス事業者の代表者は、個人情報の適切な保護を維持するために、少なくとも年1回以上個人情報保護マネジメントシステムを見直さなければならない。

**2.**　情報サービス事業者の代表者による見直しにおいては、次の事項を考慮しなければならない。

(1) 監査及び個人情報保護マネジメントシステムの運用状況に関する報告
(2) 苦情を含む外部からの意見
(3) 前回までの見直しの結果に対するフォローアップ
(4) 個人情報の取扱いに関する法令、国の定める指針その他の規範の改正状況
(5) 社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化
(6) 情報サービス事業者の事業領域の変化
(7) 情報サービス事業者の内外から寄せられた改善のための提案

## 第7章　罰　則

**（罰則）**

**第42条**　情報サービス事業者は、第10条により策定した内部規程に違反した従業者に対して、就業規則（就業規則、役員就業規則その他服務に関する規定を含む。）に基づき懲戒を行わなければならない。

## 附　則

このガイドラインの改廃は、プライバシーマーク審査会において行い、理事会の承認を得るものとする。

制定：1989年(平成元年) 7月26日　第40回理事会承認／1989年(平成元年) 7月26日施行
改定：1997年(平成 9年)11月26日第116回理事会承認／1997年(平成 9年)11月26日施行
2000年(平成12年) 5月10日第140回理事会承認／2000年(平成12年) 5月10日施行
2006年(平成18年) 5月17日第199回理事会承認／2006年(平成18年) 6月22日施行