ICS 35.040
L80

中 華 人 民 共 和 国 国 家 標 準

GB/T 35273—2020
GB/T 35273-2017 から差替え

情報安全技術　個人情報安全規範

Information security technology — Personal information security specification

（学習参考用）

2020-03-06 発布　　2020-10-01 実施

国家市場監督管理総局
発布
国家標準化管理委員会

目　　次

（日訳省略）

前　　文

（日訳省略）

序　　言

（日訳省略）

情報安全技術　個人情報安全規範

1　範囲

本標準は、収集、保存、使用、共有、譲渡、公開開示、削除等の個人情報処理活動の展開にあたり遵守すべき原則及び安全要求を定めている。

本標準は、各種組織による個人情報処理活動の規範化に適用され、主管監督管理部門、第三者評価機構等の組織が個人情報処理活動に対して監督、管理及び評価を行う際にも適用される。

2　規範的引用文書

以下の文書は、本文書の応用にとって必要不可欠なものである。日付が記載された引用文書については、日付が記載されたバージョンのみが本文書に適用される。日付が記載されていない引用文書については、その最新バージョン（全ての追補を含む。）が本文書に適用される。

GB/T 25069—2010　情報安全技術　用語

3　用語及び定義

GB/T 25069—2010 に定められた用語及び定義並びに次に掲げる用語及び定義が本文書に適用される。

3.1

個人情報　personal information

電子又はその他の方式により記録された、単独で、又はその他の情報と結びついて特定の自然人の身分を識別し、又は特定の自然人の活動状況を反映することができる各種の情報をいう。

注 1：個人情報には、氏名、生年月日、身分証書番号、個人生体識別情報、住所、通信連絡方法、通信記録及び内容、アカウントパスワード、財産情報、信用調査情報、移動軌跡、宿泊情報、健康生理情報、取引情報等を含む。

注 2：個人情報の判定方法及び類型については、付属文書 A を参照。

注 3：個人情報管理者が個人情報又はその他の情報の加工処理を通じて作成した情報（例：ユーザプロファイル又は特徴タグ）は、単独で、又はその他の情報と結びついて特定の自然人の身分を識別し、又は特定の自然人の活動状況を反映することができる場合には、個人情報に該当する。

3.2

機微な個人情報　personal sensitive information

一旦漏洩され、不法に提供され、又は濫用されると、人身及び財産の安全に危害を及ぼす虞があり、個人の名誉及び心身の健康が損害又は差別的待遇等を受けることに極めてつながりやすい個人情報をいう。

注 1：機微な個人情報には、身分証書番号、個人生体識別情報、銀行口座、通信記録及び内容、財産情報、信用調査情報、移動軌跡、宿泊情報、健康生理情報、取引情報、14 歳以下の児童の個人情報等を含む。

注 2：機微な個人情報の判定方法及び類型については、付属文書 B を参照。

注 3：個人情報管理者が個人情報又はその他の情報の加工処理を通じて作成した情報は、一旦漏洩され、不法に提供され、又は濫用されると、人身及び財産の安全に危害を及ぼす虞があり、個人の名誉及び心身の健康が損害又は差別的待遇等を受けることに極めてつながりやすい場合には、機微な個人情報に該当する。

3.3

個人情報主体　personal information subject

個人情報により識別され、又はこれに関連付けられる自然人をいう。

3.4

個人情報管理者　personal information controller

個人情報処理の目的、方式等を決定する能力を有する組織又は個人をいう。

3.5

収集　collect

個人情報の管理権を取得する行為をいう。

注 1：個人情報主体による自発的な提供、個人情報主体とのインタラクション又は個人情報主体の行為の記録等を通じた自動採取行為、及び公開情報の共有、譲渡、採集等を通じた個人情報の間接的入手等の行為が含まれる。

注 2：製品又はサービスの提供者がツールを提供して個人情報主体の使用に供した場合において、提供者が個人情報へのアクセスを行わなかったときは、本標準にいう「収集」に該当しない。例えば、オフラインナビゲーションソフトウェアが端末において個人情報主体の位置情報を入手した後、ソフトウェア提供者に送り返さない場合は、個人情報主体の位置情報の収集に該当しない。

3.6

明示の同意　explicit consent

個人情報主体が書面、口頭等の方式を通じて紙媒体若しくは電子形式による表明を自発的に行い、又は肯定的動作を自主的に行い、自身の個人情報への特定の処理の実施について明確な授権をなす行為をいう。

注：肯定的動作には、個人情報主体による「同意する」、「登録」、「送信」又は「電話発信」への自発的なチェック入力又は自発的なクリック、自発的な記入又は提供等が含まれる。

3.7

授権同意　consent

個人情報主体が自身の個人情報への特定の処理の実施について明確な授権をなす行為をいう。

注：積極的行為を通じて授権をなすこと（即ち明示の同意）、又は消極的不作為を通じて授権をなすこと（例：情報採取エリア内の個人情報主体が情報収集行為を告知された後に当該エリアを離れないこと）が含まれる。

3.8

ユーザプロファイリング　user profiling

個人情報の収集・集約・分析を通じて、ある特定の自然人の個人的な特徴（例：職業、経済、健康、教育、個人的嗜好、信用、行為等の方面）に対し分析又は予測を行い、その個人の人物像を作成する過程をいう。

注：特定の自然人の個人情報を直接使用して当該自然人の人物像を作成することは、「直接的ユーザプロファイリング」という。特定の自然人以外に由来する個人情報（例：当該自然人が所属するグループのデータ）を使用して当該自然人の人物像を作成することは、「間接的ユーザプロファイリング」という。

3.9

個人情報安全影響評価　personal information security impact assessment

個人情報処理活動に対し、その法規適合度を検査して、個人情報主体の適法な権益に損害をもたらす当該活動の各種リスクを判断し、及び個人情報主体の保護に用いられる各措置の有効性を評価する過程をいう。

3.10

削除　delete

日常業務機能の実現に関係するシステムにおいて個人情報を取り除く行為で、当該個人情報の検索・アクセスが不可能な状態を維持させることをいう。

3.11

公開開示　public disclosure

社会又は不特定の集団に情報を公表する行為をいう。

3.12

譲渡　transfer of control

個人情報管理権をある管理者から別の管理者に移転させる過程をいう。

3.13

共有　sharing

個人情報管理者がその他の管理者に個人情報を提供し、かつ、双方が個人情報に対し独立した管理権をそれぞれ保有する過程をいう。

3.14

匿名化　anonymization

個人情報への技術的処理を通じて、個人情報主体が識別又は関連付けられることを不可能にし、かつ、処理後の情報を復元不能にする過程をいう。

注：個人情報が匿名化処理を経た後に得られた情報は、個人情報に該当しない。

3.15

非識別化　de-identification

個人情報への技術的処理を通じて、追加的な情報に依拠しない状況では、個人情報主体について識別又は関連付けできないようにさせる過程をいう。

注：非識別化は、個体を基礎として確立され、個体という粒度を保持しながら、仮名、暗号化、ハッシュ関数等の技術的手段を用い、個人情報についての識別子を置き代えるものである。

3.16

パーソナライズド表示　personalized display

特定の個人情報主体のウェブ閲覧履歴、趣味趣向、消費記録及び習慣等の個人情報に基づいて当該個人情報主体に情報コンテンツを表示し、商品又はサービスのサーチ結果を提供する等の活動をいう。

3.17

業務機能　business function

個人情報主体の具体的な使用ニーズを満たすサービス類型をいう。

注：例えば、地図ナビゲーション、オンライン配車予約、インスタントメッセージング、オンラインコミュニティ、オンライン決済、ニュース情報、ネットショッピング、宅配便、交通チケットサービス等。

4　個人情報安全基本原則

個人情報管理者は、個人情報処理活動を展開する場合には、適法・正当・必要の原則を遵守しなければならない。具体的には、以下のものが含まれる。

a) 権限・責任一致——技術的措置及びその他必要な措置を講じて個人情報の安全を保障し、その個人情報処理活動が個人情報主体の適法な権益にもたらす損害に責任を負う。
b) 目的明確化——明確、明瞭かつ具体的な個人情報の処理目的を備える。
c) 同意選択——個人情報主体に個人情報処理の目的、方式、範囲等の規則を明示し、授権同意を求める。
d) 必要最小限——個人情報主体が授権同意した目的を満たすのに必要な最低限の個人情報の類型及び数のみを処理する。目的達成後は、個人情報を遅滞なく削除しなければならない。
e) 公開透明——明確でわかりやすく、及び合理的な方式にて個人情報処理の範囲、目的、規則等を公開し、かつ、外部の監督を受ける。
f) セキュリティ確保——直面するセキュリティリスクに対応したセキュリティ能力を備え、かつ、十分な管理措置及び技術的手段を講じて、個人情報の機密性、完全性及び可用性を保護する。

g) 主体関与——自身の個人情報の照会・訂正・削除、授権同意の撤回、アカウント抹消、苦情申立て等をすることができる方法を個人情報主体に提供する。

5 個人情報の収集

5.1 個人情報収集の適法性

個人情報管理者に対する要求には、以下のものが含まれる。

a) 欺罔・誘導・誤導の方式をもって個人情報を収集しないものとする。
b) 製品又はサービスが備える個人情報収集機能を隠蔽しないものとする。
c) 不法なルートから個人情報を入手しないものとする。

5.2 個人情報収集の必要最小限

個人情報管理者に対する要求には、以下のものが含まれる。

a) 収集する個人情報の類型は、製品又はサービスの業務機能の実現と直接の関連を有していなければならない。「直接の関連」とは、上記の個人情報の関与がなければ、製品又はサービスの機能が実現不可能であることをいう。
b) 個人情報の自動採取の頻度は、製品又はサービスの業務機能の実現に必要とされる最低の頻度でなければならない。
c) 間接的に入手する個人情報の数は、製品又はサービスの業務機能の実現に必要とされる最低限の数でなければならない。

5.3 複数の業務機能の自主的な選択

個人情報収集を必要とする複数の業務機能を製品又はサービスが提供する場合には、個人情報管理者は、製品又はサービスによって提供される業務機能及び相応の個人情報収集要請の受入れを個人情報主体の自主的な意向に背いて強要しないものとする。個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報主体が申請又は使用していない業務機能による個人情報収集の一括受入れ及び授権同意を、製品又はサービスの各業務機能の抱合せ方式を通じて当該個人情報主体に要請しないものとする。
b) 個人情報主体が自主的に行った肯定的動作（例：自発的なクリック、チェック入力、記入等）を、製品又はサービスに係る特定の業務機能の作動条件としなければならない。個人情報管理者は、個人情報主体が当該業務機能を作動させた後に限って個人情報の収集を開始しなければならない。
c) 業務機能の終了又はログアウトのルート又は方式は、個人情報主体が業務機能の使用を選択するルート又は方式と同様に簡便でなければならない。個人情報主体が特定の業務機能について終了又はログアウトを選択した後、個人情報管理者は、当該業務機能の個人情報収集活動を停止しなければならない。
d) 個人情報主体が使用に授権同意せず、特定の業務機能を終了又はログアウトした場合には、個人情報主体による授権同意を頻繁に求めないものとする。
e) 個人情報主体が使用に授権同意せず、特定の業務機能を終了又はログアウトした場合に、個人情報主体が自主的に使用を選択するその他の業務機能を一

時停止したり、又はその他の業務機能のサービス品質を落としたりしないものとする。

f) サービス品質の改善、ユーザエクスペリエンスの向上、新製品の研究開発、安全性の強化等のみを理由として、個人情報収集に同意するよう個人情報主体に強制的に要求してはならない。

5.4　個人情報収集時の授権同意

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報を収集する場合には、個人情報を収集・使用する目的、方式及び範囲等の規則を個人情報主体に告知し、かつ、個人情報主体による授権同意を取得しなければならない。

注 1：個人情報を収集・使用する業務機能を製品又はサービスが 1 つしか提供しない場合には、個人情報管理者は、個人情報保護ポリシーの形式を通じて、個人情報主体への告知を実現することができる。個人情報を収集・使用する業務機能を製品又はサービスが複数提供する場合には、個人情報管理者は、特定の個人情報の収集を実際に開始する際に、個人情報保護ポリシーの他、当該個人情報を収集・使用する目的、方式及び範囲を個人情報主体に提供し、もって個人情報主体が具体的な授権同意を行う前に自身への具体的な影響を十分に考慮することができるようにするのが適当である。

注 2：5.3 及び a)の要求に適合する実現方法については、付属文書 C を参考とすることができる。

b) 機微な個人情報を収集する前には、個人情報主体による明示の同意を取得しなければならず、かつ、個人情報主体による明示の同意が、当該主体が十分な情報を与えられた上で自主的になした、具体的かつ明瞭明確な意向の表示であるよう確保しなければならない。

c) 個人生体識別情報を収集する前には、個人生体識別情報を収集・使用する目的、方式及び範囲並びに保存期間等の規則を個別で個人情報主体に告知し、かつ、個人情報主体による明示の同意を取得しなければならない。

注：個人生体識別情報には、個人の遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認識の特徴点等が含まれる。

d) 14 歳以上の未成年者の個人情報を収集する前には、未成年者又はその保護者による明示の同意を取得しなければならず、14 歳未満である場合には、その保護者による明示の同意を取得しなければならない。

e) 個人情報を間接的に入手する場合、

1) 個人情報の出所を説明するよう個人情報提供者に要求し、かつ、当該個人情報の出所の適法性について確認を行わなければならない。

2) 個人情報提供者が既に取得している、個人情報処理に係る授権同意の範囲（使用目的、個人情報主体が譲渡、共有、公開開示及び削除に授権同意しているか否か等を含む。）を把握しなければならない。

3) 業務展開にあたって行う必要のある個人情報処理活動が、取得済の授権同意の範囲を逸脱しているときは、個人情報入手後の合理的な期間内又は個人情報を処理する前において、個人情報主体による明示の同意を取

得するか、又は個人情報提供者を通じて個人情報主体による明示の同意を取得しなければならない。

5.5　個人情報保護ポリシー

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報保護ポリシーを制定しなければならない。内容には以下のものが含まれていなければならないが、これらに限らない。
   1) 個人情報管理者の基本的な状況（主体身分及び連絡先を含む。）
   2) 個人情報を収集・使用する業務機能及び各業務機能がそれぞれ収集する個人情報の類型。機微な個人情報に関係する場合には、明確に表記するか、又は強調表示する必要がある。
   3) 個人情報の収集方式、保存期間、データの国外移転に関係する状況等の個人情報処理規則
   4) 個人情報を対外的に共有、譲渡及び公開開示する目的、関係する個人情報の類型、個人情報を受領する第三者の類型並びにそれぞれの安全責任及び法的責任
   5) 個人情報主体の権利及び実現メカニズム（例：照会方法、訂正方法、削除方法、アカウントの抹消方法、授権同意の撤回方法、個人情報副本の入手方法、情報システムの自動意思決定結果について苦情申立てを行う方法等）
   6) 個人情報の提供後に存在する可能性のあるセキュリティリスク及び個人情報を提供しなかった場合に生じる可能性のある影響
   7) 遵守する個人情報安全基本原則、備えているデータセキュリティ能力並びに講じている個人情報安全保護措置、必要なときに公開することのできるデータセキュリティ及び個人情報保護に関連する法規適合証明
   8) 個人情報主体からの問合せ及び苦情申立てを処理するルート及びメカニズム並びに外部の紛争解決機構及び連絡先
b) 個人情報保護ポリシーが告知する情報は、真実・正確・完全でなければならない。
c) 個人情報保護ポリシーの内容は、明瞭でわかりやすく、通用的な言語習慣に合致したもので、標準化された数字、図等を用い、多義的な言葉の使用を避けなければならない。
d) 個人情報保護ポリシーは、公に発表し、かつ、アクセスが容易でなければならない（例：ウェブサイトのトップページ、モバイルインターネットアプリケーションプログラムのインストールページ、付属文書 C 中のインタラクティブインターフェース又はインタラクションデザイン等の目立つ位置にリンクを設置する。）。
e) 個人情報保護ポリシーは、個人情報主体に逐一送付しなければならない。コストが高すぎる場合又は著しく困難である場合には、公告の形式にて発表することができる。
f) a)に記載された事項に変化が生じた場合には、個人情報保護ポリシーを遅滞

なく更新し、かつ、個人情報主体に新たに告知しなければならない。

注 1：組織は習慣的に個人情報保護ポリシーを「プライバシーポリシー」と命名したり、又はその他の名称をつけたりするが、その内容は個人情報保護ポリシーの内容と一致させるのが適当である。

注 2：個人情報保護ポリシーの内容については、付属文書 D を参考とすることができる。

注 3：個人情報主体が製品又はサービスを初めて起動し、アカウント登録をする等の場合においては、ポップアップウィンドウ等の形式を通じて個人情報保護ポリシーの主な内容又は中心的な内容を当該個人情報主体に進んで提示し、個人情報主体が当該製品又はサービスの個人情報処理範囲及び規則を理解し、かつ、当該製品又はサービスの使用を継続するか否かを決定することをサポートするのが適当である。

5.6　授権同意取得の例外

以下の場合において、個人情報管理者は、個人情報の収集・使用にあたり個人情報主体による授権同意を取得する必要がない。

a) 法律法規に定められた義務の個人情報管理者による履行に関連する場合
b) 国家の安全及び国防上の安全に直接関連する場合
c) 公共の安全、公衆衛生及び重大な公共の利益に直接関連する場合
d) 刑事捜査、提訴、裁判及び判決執行等に直接関連する場合
e) 個人情報主体又はその他の個人の生命、財産等の重大で適法な権益の維持の為であるにもかかわらず、本人による授権同意を得ることが困難である場合
f) 関係する個人情報が個人情報主体自ら社会公衆に公開したものである場合
g) 個人情報主体の要求に基づき契約を締結及び履行するのに必要である場合

注：個人情報保護ポリシーの主な機能は、個人情報管理者による個人情報の収集・使用の範囲及び規則を公開することであり、これを契約であるとみなすことは適切ではない。

h) 適法に公開開示された情報の中から個人情報を収集する場合（例：適法な報道、政府の情報公開等のルート）
i) 提供する製品又はサービスの安全かつ安定的な運営の維持に必要である場合（例：製品又はサービスの不具合の発見・対処）
j) 個人情報管理者が報道単位であり、かつ、その適法な報道の展開に必要である場合
k) 個人情報管理者が学術研究機構であり、公共の利益の観点から統計又は学術研究を展開するのに必要で、かつ、当該機構が学術研究又は記述の結果を対外的に提供するときに、結果中に含まれる個人情報に対し非識別化処理を行う場合

6　個人情報の保存

6.1　個人情報保存期間の最小化

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報保存期間は、個人情報主体が使用権限を付与した目的の実現に必要な最短期間としなければならない。但し、法律法規に別段の定めがある場合

又は個人情報主体が別途授権同意する場合を除く。

b) 上記の個人情報保存期間を超過した後は、個人情報に対し削除又は匿名化処理を行わなければならない。

6.2　非識別化処理

個人情報の収集後、個人情報管理者は、直ちに非識別化処理を行い、かつ、技術面及び管理面での措置を講じて、個人の復元識別に用いることのできる情報と非識別化後の情報とを分けて保存し、かつ、アクセス及び使用の権限管理を強化することが適当である。

6.3　機微な個人情報の送信及び保存

個人情報管理者に対する要求には、以下のものが含まれる。

a) 機微な個人情報を送信及び保存する場合には、暗号化等の安全措置を採用しなければならない。

注：暗号技術を採用する場合には、暗号管理に関連する国家標準を遵守することが適当である。

b) 個人生体識別情報は、個人身分情報と分けて保存しなければならない。

c) 原則として、個人生体識別に係る原始情報（例：検体、画像等）は保存しないものとする。講じることのできる措置には以下のものが含まれるが、これらに限らない。

1) 個人生体識別情報の要約情報のみを保存する。

2) 採取端末において個人生体識別情報を直接使用し、身分識別、認証等の機能を実現する。

3) 顔認識の特徴点、指紋、掌紋、虹彩等を使用して身分識別、認証等の機能を実現した後、個人生体識別情報を抽出することのできる原始画像を削除する。

注 1：要約情報は、通常の場合、不可逆性を有しており、原始情報まで遡ることはできない。

注 2：法律法規に定められた義務の個人情報管理者による履行に関連する場合を除く。

6.4　個人情報管理者による運用停止

個人情報管理者がその製品又はサービスの運用を停止する場合には、

a) 個人情報の継続的な収集を遅滞なく停止しなければならない。

b) 運用停止の通知を逐一送付又は公告の形式にて個人情報主体に知らせなければならない。

c) その保有する個人情報に対し削除又は匿名化処理を行わなければならない。

7　個人情報の使用

7.1　個人情報アクセスコントロール措置

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報へのアクセス権限を付与されている人員に対し、最小権限の付与というアクセスコントロールポリシーを確立して、職責に求められる必要最小限の個人情報にのみアクセスすることができるようにし、かつ、職責完了に

必要な最低限のデータ操作権限のみを備えさせるようにしなければならない。

b) 個人情報に対する重要な操作に内部審査承認フローを設ける（大量の修正、コピー、ダウンロード等の重要な操作を行う場合）。

c) 安全管理者、データオペレーター及び監査人の役割に対し分離設定を行う。

d) 業務上の必要性のために、特定の人員に授権し、権限を超えて個人情報を処理させる必要が確かにある場合には、個人情報保護責任者又は個人情報保護業務機構による審査承認を経て、かつ、書面記録に残さなければならない。

注：個人情報保護責任者又は個人情報保護業務機構の確定については、11.1 を参照。

e) 機微な個人情報に対するアクセス、修正等の操作行為については、役割権限に対するコントロールを基礎とし、業務フローの必要性に従って操作権限の発動に及ぶようにするのが適当である（例：顧客からの苦情申立てを受けた場合に限り、苦情申立処理人員は当該個人情報主体の関連情報にアクセスすることができる。）。

7.2　個人情報の表示制限

インターフェースを通じた個人情報の表示に及ぶ場合（例：ディスプレイスクリーン及び紙面）には、個人情報管理者は、表示する必要のある個人情報に対して非識別化処理等の措置を講じ、表示プロセスにおける個人情報の漏洩リスクを低減させることが適当である（例：個人情報表示の際に、内部の授権を受けていない人員及び個人情報主体以外のその他の人員が授権を経ずに個人情報を入手することを防ぐ。）。

7.3　個人情報の使用目的の制限

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報を使用する際には、個人情報収集時に表明した目的と直接的又は合理的な関連を有する範囲を逸脱しないものとする。業務上の必要性により、上記の範囲を逸脱して個人情報を使用する必要が確かにある場合には、個人情報主体による明示の同意を再度取得しなければならない。

注：収集した個人情報を学術研究又は自然、科学、社会、経済等の現象の全体的な状態についての記述を導き出すために用いることは、収集の目的と合理的な関連を有する範囲内に該当する。但し、学術研究又は記述の結果を対外的に提供する場合には、結果中に含まれる個人情報に非識別化処理を行う必要がある。

b) 収集した個人情報に加工処理を行って生じた情報が、単独で、又はその他の情報と結びついて特定の自然人の身分を識別し、又は特定の自然人の活動状況を反映することができる場合には、当該情報を個人情報と認定しなければならない。当該情報に対する処理は、個人情報収集時に取得した授権同意の範囲を遵守しなければならない。

注：加工処理をして生じた個人情報が機微な個人情報に該当する場合には、当該情報に対する処理は、機微な個人情報に対する要求に適合させる必要がある。

7.4　ユーザプロファイルの使用制限

個人情報管理者に対する要求には、以下のものが含まれる。

a) ユーザプロファイルにおける個人情報主体についての特徴点記述は、
   1) 猥褻、色情、賭博、迷信、恐怖及び暴力の内容を含まないものとする。
   2) 民族、人種、宗教、障害、疾病に対する差別的な内容を表現しないものとする。

b) 業務運営又は対外業務提携においてユーザプロファイルを用いる場合には、
   1) 公民、法人及びその他組織の適法な権益を侵害しないものとする。
   2) 国家の安全、栄誉及び利益に危害を及ぼし、国家政権の転覆及び社会主義制度の打倒を扇動し、国家の分裂及び国家統一の破壊を扇動し、テロリズム及び過激主義を宣揚し、民族憎悪及び民族差別を宣揚し、暴力的な情報及び猥褻・色情情報を流布し、虚偽の情報を捏造・流布して経済秩序及び社会秩序を攪乱しないものとする。

c) 個人情報主体が授権同意した使用目的を実現するために必要である場合を除き、個人情報を使用する際には、身分を明確に指し示すものを除去し、特定の個人の高精度な絞込みを回避させなければならない（例：個人の信用状況を正確に評価するためには直接的ユーザプロファイルを用いることができるが、商業広告配信目的に用いる場合には間接的ユーザプロファイルを用いるのが適当である。）。

7.5 パーソナライズド表示の使用

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報主体に業務機能を提供する過程においてパーソナライズド表示を使用する場合には、パーソナライズド表示の内容と非パーソナライズド表示の内容とを明白に区別しなければならない。

注：明白な区別の方式には「定推（ターゲティング配信）」等の文言の明記、又は異なる欄・スレッド・ページを通じた別々の表示等が含まれるが、これらに限らない。

b) 個人情報主体に電子商取引サービスを提供する過程において、消費者の趣味趣向、消費習慣等の特徴に基づき商品又はサービスのサーチ結果に係るパーソナライズド表示を当該消費者に提供する場合には、その個人的な特徴に焦点を定めていない選択肢を当該消費者に同時に提供しなければならない。

注：個人情報主体が選択した特定の地理的位置に基づき表示及びサーチ結果のソートを行いながら、個人情報主体の身分ごとに異なる内容及びサーチ結果順の表示をしないという場合には、その個人的な特徴に焦点を定めていない選択肢に該当する。

c) 個人情報主体にニュース情報サービスを配信する過程においてパーソナライズド表示を使用する場合には、
   1) パーソナライズド表示モードをオフ又は終了とするシンプルかつ直観的な選択肢を個人情報主体に提供しなければならない。
   2) 個人情報主体がパーソナライズド表示モードのオフ又は終了を選択した際に、ターゲティング配信活動の基礎とした個人情報を削除又は匿名化する選択肢を個人情報主体に提供しなければならない。

d) 個人情報主体に業務機能を提供する過程においてパーソナライズド表示を使用する場合には、パーソナライズド表示が依拠する個人情報（例：タグ、プ

ロファイルのディメンション等）に対する個人情報主体の自主管理メカニズムを確立し、パーソナライズド表示の関連性の程度を個人情報主体が調整制御する能力を保障することが適当である。

7.6　異なる業務目的に基づいて収集した個人情報の集約・融合

個人情報管理者に対する要求には、以下のものが含まれる。

a)　7.3 の要求を遵守しなければならない。

b)　集約・融合後に個人情報が用いられる目的に基づいて、個人情報安全影響評価を展開し、有効な個人情報保護措置を講じなければならない。

7.7　情報システム自動意思決定メカニズムの使用

個人情報管理者の業務運営で使用される情報システムが自動意思決定メカニズムを備え、かつ、個人情報主体の権益に著しい影響をもたらすことができる場合（例：個人の信用調査及び貸付限度額を自動で決定する、又は面接者の自動選考に用いられる等）には、

a)　計画設計段階又は初回使用前において個人情報安全影響評価を展開し、かつ、評価結果に基づいて有効な個人情報主体の保護措置を講じなければならない。

b)　使用の過程において、個人情報安全影響評価を定期的に（少なくとも毎年 1 回）展開し、かつ、評価結果に基づいて個人情報主体の保護措置を改善しなければならない。

c)　自動意思決定結果を対象とした苦情申立てルートを個人情報主体に提供し、かつ、自動意思決定結果に対する人力での再確認に対応しなければならない。

8　個人情報主体の権利

8.1　個人情報の照会

個人情報管理者は、次に掲げる情報の照会方法を個人情報主体に提供しなければならない。

a)　自身が保有する、当該主体に関する個人情報又は個人情報の類型

b)　上記の個人情報の出所及びそれを用いる目的

c)　上記の個人情報を既に取得した第三者の身分又は類型

注：自身が自発的に提供したのではない個人情報の照会を個人情報主体が申し入れた場合には、個人情報管理者は、請求に対応しないことで個人情報主体の適法な権益にもたらされるおそれのあるリスク及び損害、並びに技術的実現可能性、請求実現のコスト等の要素を総合的に考慮した上で、対応するか否かの決定を下し、かつ、説明を与えることができる。

8.2　個人情報の訂正

個人情報主体が個人情報管理者の保有する当該主体の個人情報について、誤りがあること又は不完全であることを発見した場合には、個人情報管理者は、情報の訂正又は補足の請求方法を当該個人情報主体に提供しなければならない。

8.3　個人情報の削除

個人情報管理者に対する要求には、以下のものが含まれる。

a) 以下の事由に適合し、個人情報主体が削除を要求する場合には、個人情報を遅滞なく削除しなければならない。
   1) 個人情報管理者が法律法規の規定に違反して個人情報を収集・使用した場合
   2) 個人情報管理者が個人情報主体との約定に違反して個人情報を収集・使用した場合

b) 個人情報管理者が法律法規の規定に違反し、又は個人情報主体との約定に違反して第三者に個人情報を共有・譲渡し、かつ、個人情報主体が削除を要求した場合には、個人情報管理者は、直ちに共有・譲渡行為を停止し、かつ、遅滞なく削除するよう第三者に通知しなければならない。

c) 個人情報管理者が法律法規の規定に違反し、又は個人情報主体との約定に違反して個人情報を公開開示し、かつ、個人情報主体が削除を要求した場合には、個人情報管理者は、直ちに公開開示行為を停止し、かつ、通知を出して、相応の情報を削除するよう関連する受領者に要求しなければならない。

8.4　個人情報主体による授権同意の撤回

個人情報管理者に対する要求には、以下のものが含まれる。

a) 自身の個人情報の収集・使用に係る授権同意を撤回する方法を個人情報主体に提供しなければならない。授権同意の撤回後、個人情報管理者は、相応の個人情報を後で再処理しないものとする。

b) 自身の個人情報に基づいて配信される商業広告の受領を個人情報主体が拒絶する権利を保障しなければならない。個人情報を対外的に共有、譲渡又は公開開示する場合には、授権同意を撤回する方法を個人情報主体に提供しなければならない。

注：授権同意の撤回は、撤回前の授権同意に基づく個人情報の処理に影響しない。

8.5　個人情報主体によるアカウント抹消

個人情報管理者に対する要求には、以下のものが含まれる。

a) アカウント登録を通じて製品又はサービスを提供する個人情報管理者は、個人情報主体にアカウントの抹消方法を提供しなければならず、かつ、その方法は簡便かつ操作しやすいものであること。

b) アカウント抹消請求の受理後、人力での処理が必要な場合には、約束の期限内（15 業務日を超えない。）に審査及び処理を完了させなければならない。

c) 抹消の過程において身分確認を行う必要がある場合には、個人情報主体に再度の提供を要求する個人情報の類型は、登録、使用等のサービスプロセスで収集した個人情報の類型より多くならないものとする。

d) 抹消の過程において、不合理な条件を設け、又は追加的な要求を打ち出して個人情報主体の義務を増やさないものとする（例：1 つのアカウントの抹消を複数の製品又はサービスの抹消とみなし、抹消の必要条件として精確な過去の操作記録の記入を個人情報主体に要求する等。）。

注 1：複数の製品又はサービス間に必要な業務関連関係がある場合（例：ある製品又はサービス

のアカウントを一旦抹消すると、その他の製品若しくはサービスの必要な業務機能が実現不可能となり、又はサービスの品質の著しい低下につながる場合）には、個人情報主体に詳細な説明を行う必要がある。

注 2：製品又はサービスが独立したアカウント体系を有しない場合には、当該製品又はサービスのアカウント以外のその他の個人情報に対して削除を行い、かつ、アカウント体系と製品又はサービスとの関連を切断する等の措置を講じて抹消を実現することができる。

e) アカウント抹消の過程において、機微な個人情報を収集して身分を確認する必要がある場合には、機微な個人情報収集後についての処理措置を明確にしなければならない（例：目的達成後、直ちに削除又は匿名化処理をする等）。

f) 個人情報主体がアカウントを抹消した後は、遅滞なくその個人情報を削除し、又は匿名化処理をしなければならない。法律の規定により個人情報を保管する必要がある場合には、当該個人情報を日常の業務活動中に再度用いることはできない。

8.6　個人情報主体による個人情報副本の入手

個人情報主体からの請求に基づき、個人情報管理者は、以下の類型の個人情報副本の入手方法を個人情報主体に提供し、又は技術的に実行可能であるという前提の下で、以下の類型の個人情報の副本を個人情報主体が指定する第三者に直接送信することが適当である。

a) 本人の基本的資料及び身分情報

b) 本人の健康生理情報及び教育就労情報

8.7　個人情報主体からの請求への対応

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報主体の身分認証後、個人情報主体が 8.1～8.6 に基づき提出した請求に遅滞なく対応しなければならず、30 日内又は法律法規に定められた期間内に回答及び合理的な説明を行い、かつ、外部の紛争解決ルートを個人情報主体に告知しなければならない。

b) インタラクティブページ（例：ウェブサイト、モバイルインターネットアプリケーションプログラム、クライアントサイドソフトウェア等）を採用して製品又はサービスを提供する場合には、簡便なインタラクティブページを直接設置して機能又は選択肢を提供し、個人情報主体によるそのアクセス、訂正、削除、授権同意の撤回、アカウント抹消等の権利のオンライン上での行使に便宜を図ることが適当である。

c) 合理的な請求に対しては、原則として費用を徴収しない。但し、一定の期間内に何度も繰り返される請求に対しては、状況に応じて一定のコスト費用を徴収することができる。

d) 個人情報主体からの請求を直接実現するにあたり多額のコストを費やす必要がある場合又はその他著しい困難が存在する場合には、個人情報管理者は、個人情報主体に代替方法を提供し、もって個人情報主体の適法な権益を保障しなければならない。

e) 以下の場合においては、個人情報主体が 8.1～8.6 に基づいて提出した請求に

対応しないことができる。

1) 法律法規に定められた義務の個人情報管理者による履行に関連する場合
2) 国家の安全及び国防上の安全に直接関連する場合
3) 公共の安全、公衆衛生及び重大な公共の利益に直接関連する場合
4) 刑事捜査、提訴、裁判及び判決執行等に直接関連する場合
5) 個人情報主体について、主観的悪意の存在又は権利の濫用を示す十分な証拠を個人情報管理者が有する場合
6) 個人情報主体又はその他の個人の生命、財産等の重大で適法な権益の維持の為であるにもかかわらず、本人による授権同意を得ることが困難である場合
7) 個人情報主体からの請求に対応することで個人情報主体又はその他の個人・組織の適法な権益が重大な損害を被ることになる場合
8) 商業秘密に関係する場合

f) 個人情報主体からの請求に対応しないことを決定した場合には、個人情報主体に当該決定の理由を告知し、かつ、個人情報主体に苦情申立てルートを提供しなければならない。

8.8　苦情申立管理

個人情報管理者は、苦情申立管理メカニズム及び苦情申立てのフォローアップフローを確立し、かつ、合理的な期間内に苦情申立てへの対応を行わなければならない。

9　個人情報の処理委託、共有、譲渡及び公開開示

9.1　処理委託

個人情報管理者が第三者に個人情報の処理を委託する場合には、以下の要求に適合していなければならない。

a) 個人情報管理者は、委託行為を行う場合には、個人情報主体による授権同意を取得済みの範囲を逸脱しないものとし、又は 5.6 に記載の状況を遵守しなければならない。
b) 個人情報管理者は、委託行為に対して個人情報安全影響評価を行い、受託者が 11.5 のデータセキュリティ能力要求に達するよう確保しなければならない。
c) 受託者は、
   1) 個人情報管理者の要求に厳格に従って個人情報を処理しなければならない。受託者は、特殊な原因により個人情報管理者の要求どおりに個人情報を処理しなかった場合には、遅滞なく個人情報管理者にフィードバックしなければならない。
   2) 受託者が再委託する必要が確かにある場合には、個人情報管理者による授権を事前に取得しなければならない。
   3) 個人情報主体が 8.1～8.6 に基づき提出した請求に、個人情報管理者に協力して対応しなければならない。

4) 受託者による個人情報処理の過程において十分な安全保護水準を提供することができず、又はセキュリティインシデントが発生した場合には、遅滞なく個人情報管理者にフィードバックしなければならない。
5) 委託関係が解除された場合には、関連する個人情報の保存を取りやめなければならない。

d) 個人情報管理者は、受託者に対し監督を行わなければならず、その方式には以下のものが含まれるがこれらに限らない。
1) 契約等の方式を通じて受託者の責任及び義務を定める。
2) 受託者に対して監査を行う。

e) 個人情報管理者は、個人情報の処理委託に係る状況を正確に記録及び保存しなければならない。

f) 個人情報管理者は、受託者が委託要求どおりに個人情報を処理していないこと又は個人情報安全保護責任を有効に履行できていないことを知り、又は発見した場合には、関連行為を停止するよう受託者に直ちに要求し、かつ、有効な救済措置（例：パスワードの変更、権限の回収、ネットワーク接続の切断等）を講じるか、又はそれを講じるよう受託者に要求して、個人情報が直面するセキュリティリスクを制御又は除去しなければならない。必要な場合には、個人情報管理者は、受託者との業務関係を終了し、かつ、個人情報管理者から取得した個人情報を遅滞なく削除するよう受託者に要求しなければならない。

9.2　個人情報の共有・譲渡

個人情報管理者は、個人情報を共有・譲渡する場合には、リスクを十分に重視しなければならない。個人情報の共有・譲渡の理由が買収、吸収合併、再編及び破産ではない場合には、以下の要求に適合していなければならない。

a) 個人情報安全影響評価を事前に展開し、かつ、評価結果に基づいて有効な個人情報主体の保護措置を講じる。

b) 個人情報の共有・譲渡の目的、データ受領者の類型及び生じる可能性のある結果を個人情報主体に告知し、かつ、個人情報主体による授権同意を事前に取得する。但し、非識別化処理を経た個人情報を共有・譲渡し、かつ、データ受領者が個人情報主体を再識別又は関連付けできないよう確保する場合を除く。

c) 機微な個人情報を共有・譲渡する前には、b）中の告知内容の他、関係する機微な個人情報の類型、データ受領者の身分及びデータセキュリティ能力についても個人情報主体に告知し、かつ、個人情報主体による明示の同意を事前に取得しなければならない。

d) 契約等の方式を通じてデータ受領者の責任及び義務を定める。

e) 個人情報の共有・譲渡に係る状況（共有・譲渡の日付、規模、目的及びデータ受領者の基本的な状況等を含む。）を正確に記録及び保存する。

f) 個人情報管理者は、データ受領者が法律法規の要求又は双方の約定に違反して個人情報を処理していることを発見した場合には、関連行為を停止するよ

うデータ受領者に直ちに要求し、かつ、有効な救済措置（例：パスワードの変更、権限の回収、ネットワーク接続の切断等）を講じ、又はその実施をデータ受領者に要求して、個人情報が直面するセキュリティリスクを制御又は除去しなければならない。必要な場合には、個人情報管理者は、データ受領者との業務関係を解除し、かつ、個人情報管理者から取得した個人情報を遅滞なく削除するようデータ受領者に要求しなければならない。

g) 個人情報の共有・譲渡によりセキュリティインシデントが発生し、個人情報主体の適法な権益に損害がもたらされた場合には、個人情報管理者は、相応の責任を負わなければならない。

h) 個人情報に対する保存、使用等に係るデータ受領者の状況及び個人情報主体の権利（例：アクセス、訂正、削除、アカウント抹消等）を個人情報主体が把握することをサポートする。

i) 個人生体識別情報は、原則として共有・譲渡しないものとする。業務上の必要性により共有・譲渡する必要が確かにある場合には、目的、関係する個人生体識別情報の類型、データ受領者の具体的な身分及びデータセキュリティ能力等を個別で個人情報主体に告知し、かつ、個人情報主体による明示の同意を取得しなければならない。

9.3　買収、吸収合併、再編及び破産時における個人情報の譲渡

個人情報管理者に買収、吸収合併、再編、破産等の変更が生じた場合において、個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報主体に関係状況を告知する。

b) 変更後の個人情報管理者は、元の個人情報管理者の責任及び義務を継続して履行しなければならず、個人情報の使用目的を変更する場合には、個人情報主体による明示の同意を新たに取得しなければならない。

c) 破産し、かつ、承継人がいない場合には、データに対し削除処理を行う。

9.4　個人情報の公開開示

個人情報は、原則として公開開示しないものとする。個人情報管理者が法律による授権を経ており、又は合理的な事由を有していて公開開示する必要が確かにある場合には、以下の要求に適合していなければならない。

a) 個人情報安全影響評価を事前に展開し、かつ、評価結果に基づいて有効な個人情報主体の保護措置を講じる。

b) 個人情報の公開開示に係る目的・類型を個人情報主体に告知し、かつ、個人情報主体による明示の同意を事前に取得する。

c) 機微な個人情報を公開開示する前には、b）中の告知内容の他、関係する機微な個人情報の内容についても個人情報主体に告知しなければならない。

d) 個人情報の公開開示に係る状況（公開開示の日付、規模、目的、公開範囲等を含む。）を正確に記録及び保存する。

e) 個人情報の公開開示により個人情報主体の適法な権益にもたらされる損害に係る相応の責任を負う。

f) 個人生体識別情報を公開開示しないものとする。
g) 我が国公民の人種、民族、政治的見解、宗教信仰等の機微な個人データに係る分析結果を公開開示しないものとする。

9.5　個人情報を共有、譲渡及び公開開示する場合における授権同意の事前取得の例外

以下の場合において、個人情報管理者は、個人情報を共有、譲渡及び公開開示するにあたり、個人情報主体による授権同意を事前に取得する必要がない。

a) 法律法規に定められた義務の個人情報管理者による履行に関連する場合
b) 国家の安全及び国防上の安全に直接関連する場合
c) 公共の安全、公衆衛生及び重大な公共の利益に直接関連する場合
d) 刑事捜査、提訴、裁判及び判決執行等に直接関連する場合
e) 個人情報主体又はその他の個人の生命、財産等の重大で適法な権益の維持の為であるにもかかわらず、本人による授権同意を得ることが困難である場合
f) 個人情報主体が自ら社会公衆に公開した個人情報
g) 適法に公開開示された情報の中から個人情報を収集する場合（例：適法な報道、政府の情報公開等のルート）

9.6　共同個人情報管理者

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報管理者と第三者が共同個人情報管理者となる場合には、個人情報管理者は、契約等の形式を通じて、満たすべき個人情報安全要求並びに個人情報の安全面で自身及び第三者がそれぞれ負うべき責任及び義務を第三者と共同で確定し、かつ、個人情報主体に対し明確に告知しなければならない
b) 第三者の身分並びに個人情報の安全面で自身及び第三者がそれぞれ負うべき責任及び義務を個人情報主体に対し明確に告知していない場合には、個人情報管理者は、第三者によって引き起こされる個人情報安全責任を引き受けなければならない。

注：個人情報管理者が製品又はサービス提供の過程において個人情報を収集するサードパーティのプラグインを配置しており（例：ウェブサイト事業者とそのウェブページ又はアプリケーションプログラムとの間に統計分析ツール若しくは SDK を配置し、又は地図 API を呼び出す。）、かつ、当該サードパーティが個人情報収集に係る授権同意を個別で個人情報主体から取得していない場合には、個人情報管理者と当該サードパーティは、個人情報収集段階において共同個人情報管理者となる。

9.7　サードパーティ接続管理

個人情報管理者が自身の製品又はサービスにおいて、個人情報収集機能を具備するサードパーティの製品又はサービスに接続し、かつ、9.1 及び 9.6 が適用されない場合には、個人情報管理者に対する要求に、以下のものが含まれる。

a) サードパーティの製品又はサービスの接続管理メカニズム及び業務フローを確立し、必要な場合には安全評価等のメカニズムを確立して接続条件を設けなければならない。

b) サードパーティの製品又はサービスの提供者と契約等の形式を通じて双方の安全責任及び実施すべき個人情報安全措置を明確にしなければならない。
c) 個人情報主体に対し、製品又はサービスがサードパーティによって提供されていることを明確に示さなければならない。
d) プラットフォームのサードパーティ接続に関係する契約及び管理記録を適切に保管して、関係当事者の閲覧に供することができるよう確保しなければならない。
e) 本標準の関連要求に基づいて個人情報収集に係る授権同意を個人情報主体から取得するようサードパーティに要求し、必要な場合にはその実現方式を確認しなければならない。
f) 個人情報主体からの請求及び苦情申立て等に対応するメカニズムを確立するようサードパーティの製品又はサービスに要求し、もって個人情報主体の照会・使用に供さなければならない。
g) サードパーティの製品又はサービスの提供者を監督して個人情報安全管理を強化しなければならず、サードパーティの製品又はサービスが安全管理要求及び責任を遂行していないことを発見した場合には是正するよう遅滞なく督促し、必要な場合には接続を停止しなければならない。
h) 製品又はサービスがサードパーティの自動化ツール（例：コード、スクリプト、インターフェース、アルゴリズムモデル、SDK、ミニプログラム等）を組み込んでいるか、又はそれに接続している場合には、以下の措置を講じることが適当である。
   1) 技術点検を展開して、当該ツールによる個人情報の収集・使用行為が約定の要求に適合するよう確保する。
   2) サードパーティが組み込み、又は接続した自動化ツールによる個人情報収集行為に対して監査を行い、約定を逸脱する行為を発見した場合には、遅滞なく接続を切断する。

9.8　個人情報の越境送信

中華人民共和国国内での運営において収集し、及び生じた個人情報が国外に提供される場合には、個人情報管理者は、国の関連規定及び関連標準の要求を遵守しなければならない。

10　個人情報セキュリティインシデントへの対処

10.1　個人情報セキュリティインシデントの緊急時対処及び報告

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報セキュリティインシデント緊急時対応案を策定しなければならない。
b) 定期的に（少なくとも毎年 1 回）内部の関係者を組織して緊急時対応研修及び緊急時訓練を行い、部署の職責並びに緊急時対処ポリシー及び規程を把握させなければならない。
c) 個人情報セキュリティインシデントの発生後、個人情報管理者は、緊急時対応案に基づいて以下の対処を行わなければならない。

1) インシデントの内容（インシデントを発見した人員、時間及び場所、関係する個人情報及び人数、インシデントが発生したシステムの名称、その他の相互接続システムに対する影響、並びに既に法執行機関又は関係部門に連絡したか否かが含まれるがこれらに限らない。）を記録する。
2) インシデントがもたらし得る影響を評価し、かつ、必要な措置を講じて事態を制御し、潜在的危険を除去する。
3) 「国家ネットワークセキュリティインシデント緊急時対応案」等の関係規定に従って遅滞なく上級に報告する。報告内容には、関係する個人情報主体の類型、数、内容、性質等の全体的な状況、インシデントがもたらし得る影響、既に講じ、又は講じようとしている対処措置、及びインシデント対処関係者の連絡先が含まれるがこれらに限らない。
4) 個人情報漏洩インシデントが個人情報主体の適法な権益に重大な危害を及ぼす虞がある場合（例：機微な個人情報の漏洩）には、10.2 の要求に従ってセキュリティインシデントの告知を実施する。

d) 関連する法律法規の変化の状況及びインシデント対処状況に基づいて緊急時対応案を遅滞なく更新する。

10.2　セキュリティインシデントの告知

個人情報管理者に対する要求には、以下のものが含まれる。

a) インシデントの関連状況を、メール、信書、電話、プッシュ通知等の方式にて、影響を受ける個人情報主体に遅滞なく告知しなければならない。個人情報主体に逐一告知することが困難である場合には、合理的かつ有効な方式を採用して公衆に関係する警告情報を公表しなければならない。
b) 告知内容には以下のものが含まれていなければならないが、これらに限らない。
1) セキュリティインシデントの内容及び影響
2) 既に講じ、又は講じようとしている対処措置
3) 個人情報主体による自主的なリスク防御及び低減に係る提案
4) 個人情報主体に提供される救済措置
5) 個人情報保護責任者及び個人情報保護業務機構の連絡先

11　組織の個人情報安全管理要求

11.1　責任部門及び責任者の明確化

個人情報管理者に対する要求には、以下のものが含まれる。

a) その法定代表者又は主要責任者が個人情報の安全に対して全面的な指導責任を負うこと（個人情報安全業務のためにヒト・カネ・モノの保障を提供すること等を含む。）を明確にしなければならない。
b) 個人情報保護責任者及び個人情報保護業務機構を任命しなければならない。個人情報保護責任者は、関連する管理業務の経歴及び個人情報保護の専門知識を有する人員が務め、個人情報処理活動に関する重要な意思決定に関与し

て組織の主要責任者に対し業務を直接報告しなければならない。

c) 以下の条件のいずれかを満たす組織は、専任の個人情報保護責任者及び個人情報保護業務機構を置き、個人情報安全業務に責任を負わせなければならない。

1) 主な業務が個人情報の処理に関係しており、かつ、従業員の規模が 200 人を上回っている場合

2) 100 万人分を超える個人情報を処理しているか、又は 12 か月内に 100 万人分を超える個人情報を処理する見通しがある場合

3) 10 万人分を超える機微な個人情報を処理している場合

d) 個人情報保護責任者及び個人情報保護業務機構の職責には以下のものが含まれていなければならないが、これらに限らない。

1) 組織内部の個人情報安全業務を全面的かつ統一的に実施し、個人情報安全に対して直接責任を負う。

2) 個人情報保護業務計画の策定を組織し、かつ、遂行を促す。

3) 個人情報保護ポリシー及び関連規程を制定、発行、実施し、及び定期的に更新する。

4) 組織が保有する個人情報リスト（個人情報の類型、数、出所、受領者等を含む。）及びアクセス権限付与ポリシーを確立、維持及び更新する。

5) 個人情報安全影響評価を展開し、個人情報保護に係る対策の提案を打ち出して、潜在的な安全上の危険が是正されるよう促す。

6) 個人情報安全研修の展開を組織する。

7) 製品又はサービスのオンラインリリース前に検査を行い、未知の個人情報収集、使用、共有等の処理行為を回避する。

8) 苦情申立て、通報の方式等の情報を公表し、かつ、苦情申立て・通報を遅滞なく受理する。

9) 安全監査を行う。

10) 監督・管理部門と連絡を取り合い、個人情報保護及びインシデント対処等の状況を知らせ、又は報告する。

e) 個人情報保護責任者及び個人情報保護業務機構に必要な資源を提供し、その独立した職責履行を保障しなければならない。

11.2　個人情報安全エンジニアリング

個人情報処理機能を有する製品又はサービスを開発する場合には、個人情報管理者は、国の関係標準に基づき、要件、設計、開発、テスト、リリース等のシステムエンジニアリングの段階において個人情報保護要求を考慮し、システム構築時に、個人情報保護措置に対する同時計画、同時構築及び同時使用を保証することが適当である。

11.3　個人情報処理活動記録

個人情報管理者は収集・使用した個人情報の処理活動記録を確立、維持及び更新することが適当であり、記録の内容は以下のものを含むことができる。

a) 関係する個人情報の類型、数、出所（例：個人情報主体からの直接収集又は間

接的入手の方式を通じた取得）

b）業務機能及び授権状況に基づいて区別した個人情報の処理目的及び使用場面、並びに処理委託、共有、譲渡、公開開示、国外移転に関係するか否か等の状況

c）個人情報処理活動の各プロセスに関連する情報システム、組織又は人員

11.4　個人情報安全影響評価の展開

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報安全影響評価制度を確立して、個人情報処理活動に存在するセキュリティリスクを評価し、かつ、これに対処しなければならない。

b) 個人情報安全影響評価は、処理活動における個人情報安全基本原則の遵守状況及び個人情報主体の適法な権益に対する個人情報処理活動の影響を主に評価しなければならず、内容には以下のものが含まれるがこれらに限らない。

1) 個人情報収集プロセスが目的明確化、同意選択、必要最小限等の原則を遵守しているか否か。

2) 個人情報処理が個人情報主体の適法な権益に不利な影響をもたらす虞があるか否か（人身及び財産の安全に危害を及ぼし得るか否か、個人の名誉及び心身の健康を損ない得るか否か、異なる待遇をもたらし得るか否か等を含む。）。

3) 個人情報安全措置の有効性

4) 匿名化又は非識別化処理後のデータセットが個人情報主体を再識別するリスク、又はその他のデータセットとの集約後に個人情報主体を再識別するリスク

5) 個人情報の共有、譲渡及び公開開示によって個人情報主体の適法な権益に生じる虞のある不利な影響

6) セキュリティインシデントが発生した場合に個人情報主体の適法な権益に生じる虞のある不利な影響

c) 製品若しくはサービスのリリース前、又は業務機能に重大な変化が生じた場合において、個人情報安全影響評価を行わなければならない。

d) 法律法規に新たな要求がある場合、ビジネスモデル、情報システム若しくは運営環境に重大な変更が生じた場合、又は重大な個人情報のセキュリティインシデントが発生した場合には、個人情報安全影響評価を行わなければならない。

e) 個人情報安全影響評価報告を作成し、かつ、これにより個人情報主体の保護措置を講じて、受け入れることができる水準までリスクを低減させる。

f) 個人情報安全影響評価報告を適切に保管して関係当事者の閲覧に供することができるよう確保し、かつ、適切な形式にて対外的に公開する。

11.5　データセキュリティ能力

個人情報管理者は、関係する国家標準の要求に基づき適当なデータセキュリティ能力を確立し、必要な管理措置及び技術的措置を遂行して、個人情報の漏洩、損壊、紛失及び改竄を防止しなければならない。

11.6　人員管理及び研修

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報処理に従事する部署の関係者と秘密保持合意を締結し、機微な個人情報に大量に接触する人員に対してバックグラウンドチェックを行い、もって当該人員の犯罪記録、信義誠実状況等を把握しなければならない。

b) 内部の個人情報処理に関係する部署ごとの安全職責を明確にし、セキュリティインシデントが発生した場合の処罰メカニズムを確立しなければならない。

c) 個人情報処理部署の関係者が部署を異動し、又は労働契約を終了する場合に、秘密保持義務を引き続き履行するよう要求しなければならない。

d) 個人情報にアクセスすることができる外部のサービス担当者が遵守すべき個人情報安全要求を明確にして、当該担当者と秘密保持合意を締結し、かつ、監督を行わなければならない。

e) 相応の内部制度及び方針を確立して、個人情報保護の指針及び要求を従業員に提示しなければならない。

f) 定期的に（少なくとも毎年 1 回）又は個人情報保護ポリシーに重大な変化が生じた場合に、個人情報処理部署の関係者に対し個人情報安全に特化した研修及び考査を展開して、個人情報保護ポリシー及び関連規程について関係者の習熟習得を確保しなければならない。

11.7　安全監査

個人情報管理者に対する要求には、以下のものが含まれる。

a) 個人情報保護ポリシー、関連規程及び安全措置の有効性に対し監査を行わなければならない。

b) 自動化監査システムを構築して個人情報処理活動をモニタリング記録しなければならない。

c) 監査過程において形成される記録は、セキュリティインシデントへの対処、緊急時対応及び事後調査に対しサポートを提供することができるものでなければならない。

d) 監査記録に対する授権を受けていないアクセス、改竄又は削除を防止しなければならない。

e) 監査過程において発見された、個人情報のルールに反した使用、濫用等の状況を遅滞なく処理しなければならない。

f) 監査記録及び保管期間は、法律法規の要求に適合していなければならない。

付属文書A
（資料性付属文書）
個人情報の例

「個人情報」とは、電子又はその他の方式により記録された、単独で、又はその他の情報と結びついて特定の自然人の身分を識別し、又は特定の自然人の活動状況を反映することができる各種の情報（例：氏名、生年月日、身分証書番号、個人生体識別情報、住所、通信連絡方法、通信記録及び内容、アカウントパスワード、財産情報、信用調査情報、移動軌跡、宿泊情報、健康生理情報、取引情報等）をいう。

ある情報が個人情報に該当するか否かを判定する場合には、以下の 2 つのルートを考慮しなければならない。1 つ目は識別、即ち情報から個人へのルートで、情報そのものの特殊性によって特定の自然人が識別されることであり、個人情報は特定の個人を識別する役割を果たすものでなければならない。2 つ目は関連付け、即ち個人から情報へのルートで、例えば既に知られている特定の自然人について、当該特定の自然人の活動中に生じた情報（例：個人位置情報、個人通話記録、個人閲覧記録等）が個人情報となる。上記 2 種類の状況のいずれかに適合する情報は、いずれも個人情報であると判定しなければならない。

表 A.1 に、個人情報の例を挙げる。

表 A.1　個人情報例示

個人基本的資料	個人の氏名、誕生日、性別、民族、国籍、家族関係、住所、個人の電話番号、E メールアドレス等
個人身分情報	身分証、軍官証、パスポート、運転免許証、勤務証、通行証、社会保険カード、居住証等
個人生体識別情報	個人の遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認識の特徴点等
オンライン身分識別表示情報	個人情報主体のアカウント、IP アドレス、個人のデジタル証明書等
個人健康生理情報	発病・治療等によって生じた個人の関連記録（例：病症、入院記録、医師指示書、検査報告、手術及び麻酔記録、看護記録、投薬記録、薬物・食物アレルギー情報、出産情報、既往歴、診療状況、家族の病歴、現病歴、感染症病歴等）及び個人の身体健康状況に関連する情報（例：体重、身長、肺活量等）
個人教育就労情報	個人の職業、役職、勤務先、学歴、学位、教育歴、職歴、研修記録、成績表等
個人財産情報	銀行口座、識別情報（パスワード）、預金情報（資金量、出入金記録等を含む。）、不動産情報、信用貸付記録、信用調査情報、取引及び消費記録、出納記録等並びに仮想通貨、仮想取引、ゲーム類引換コード等の仮想財産情報
個人通信情報	通信記録及び内容、ショートメッセージ、MMS、電子メール並びに個人の通信が記述されたデータ（一般的にメタデータという。）等
連絡先情報	アドレス帳、友人リスト、グループリスト、E メールアドレスリスト等
個人インターネット接続記録	ログを通じて保存された個人情報主体の操作記録（ウェブサイト閲覧記録、ソフトウェア使用記録、クリック記録、ブックマークリスト等を含む。）をいう。

個人常用デバイス情報	ハードウェアのシリアルナンバー、デバイスの MAC アドレス、ソフトウェアリスト、UDID（例 : IMEI/Android ID/IDFA/OpenUDID/GUID/SIM カードの IMSI 情報等）等を含む、個人の常用デバイスの基本的な状況が記述された情報をいう。
個人位置情報	移動軌跡、高精度位置情報、宿泊情報、経緯度等を含む。
その他の情報	婚姻歴、宗教信仰、性的指向、未公開の違法犯罪記録等

付属文書B
（資料性付属文書）
機微な個人情報の判定

「機微な個人情報」とは、一旦漏洩され、不法に提供され、又は濫用されると、人身及び財産の安全に危害を及ぼす虞があり、個人の名誉及び心身の健康が損害又は差別的待遇等を受けることに極めてつながりやすい個人情報をいう。通常の場合、14 歳以下の児童の個人情報及び自然人のプライバシーに関係する情報は、機微な個人情報に該当する。以下の観点から、機微な個人情報に該当するか否かを判定することができる。

漏洩：個人情報が一旦漏洩すると、個人情報主体並びに個人情報を収集・使用する組織及び機構が個人情報に対する管理能力を喪失することになり、個人情報の拡散範囲及び用途が制御不能となる。ある個人情報が漏洩した後、個人情報主体の意向に背く方式にて直接使用され、又はその他の情報との関連分析が行われて、個人情報主体の権益に重大なリスクをもたらす虞がある場合には、機微な個人情報であると判定しなければならない（例：個人情報主体の身分証の写しが他人によって携帯電話番号カードの実名登録、銀行口座の口座開設・カード発行に用いられる等）。

不法な提供：ある個人情報について、個人情報主体による授権同意の範囲外において拡散されるだけで個人情報主体の権益に重大なリスクをもたらしうる場合には、機微な個人情報であると判定しなければならない（例：性的指向、預金情報、感染症病歴等）。

濫用：ある個人情報が授権の合理的な範囲を逸脱した場合において使用されると（例：処理目的の変更、処理範囲の拡大等）、個人情報主体の権益に重大なリスクをもたらす虞があるときは、機微な個人情報であると判定しなければならない（例：個人情報主体による授権を取得していない場合において、健康情報を保険会社の営業販売及び個人保険料の高低の確定に用いる。）。

表 B.1 に、機微な個人情報の例を挙げる。

表 B.1　機微な個人情報例示

個人財産情報	銀行口座、識別情報（パスワード）、預金情報（資金量、出入金記録等を含む。）、不動産情報、信用貸付記録、信用調査情報、取引及び消費記録、出納記録等並びに仮想通貨、仮想取引、ゲーム類引換コード等の仮想財産情報
個人健康生理情報	発病・治療等によって生じた個人の関連記録（例：病症、入院記録、医師指示書、検査報告、手術及び麻酔記録、看護記録、投薬記録、薬物・食物アレルギー情報、出産情報、既往歴、診療状況、家族の病歴、現病歴、感染症病歴等）
個人生体識別情報	個人の遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認識の特徴点等
個人身分情報	身分証、軍官証、パスポート、運転免許証、勤務証、社会保険カード、居住証等
その他の情報	性的指向、婚姻歴、宗教信仰、未公開の違法犯罪記録、通信記録及び内容、アドレス帳、友人リスト、グループリスト、移動軌跡、ウェブページ閲覧記録、宿泊情報、高精度位置情報等

付属文書C
（資料性付属文書）
個人情報主体の自主的な意向を実現する方法

C.1　概要

個人情報主体の自主的な意向の保障には、①複数の業務機能を受け入れるよう個人情報主体に強要しないこと、②個人情報の収集・使用に対する個人情報主体の知る権利及び授権同意の権利を保障することという 2 つの側面が含まれる。個人情報管理者、特にモバイルインターネットアプリケーションプログラムの運営者は、以下の方式を通じてこれを実現することができる。

C.2　基本業務機能及び拡張業務機能の区別

個人情報主体の同意選択の権利を保障するには、まず製品又はサービスの基本業務機能及び拡張業務機能を区分する必要がある。区分の方法は、次のとおりである。

a) 個人情報主体が提供される製品又はサービスを選択・使用する際にそもそも期待しているもの及び最も主要なニーズに基づいて、製品又はサービスの基本業務機能の区分を確定しなければならない。

注 1：個人情報主体がある製品又はサービスを識別又は選択する理由は、個人情報管理者がその提供する製品又はサービスについて展開する市場プロモーション及びビジネスのポジショニング、製品又はサービスそのものの名称、アプリケーションストアにおける記述、その属するアプリケーション類型等の要素に主に基づいている。よって、個人情報管理者は、自身のアイデアではなく、一般の個人情報主体の上記要素に対する最も可能性の高い認識及び理解に基づいて個人情報主体の主要なニーズ及び期待されているものを確定し、基本業務機能の区分を確定しなければならない。一般に、製品又はサービスが基本業務機能を提供しない場合には、個人情報主体が当該製品又はサービスを選択し使用することはない。

注 2：製品又はサービスのイテレーション、拡張、アップデート等に伴って、基本業務機能にはそれに応じた再区分が必要となる可能性がある。個人情報管理者は、従前どおり一般の個人情報主体の最も可能性の高い認識及び理解に基づいて基本業務機能の区分を再確定することができる。但し、個人情報管理者が短期間内に、かつ広範囲にわたって基本業務機能及び拡張業務機能の区分を変更することは望ましくない。再区分後、個人情報管理者は、再度告知し、かつ、基本業務機能による個人情報の収集・使用について個人情報主体による明示の同意を取得することが適当である。

b) サービス品質の改善、個人情報主体のエクスペリエンス向上及び新製品の研究開発を単独で基本業務機能としないものとする。

c) 製品又はサービスが提供する基本業務機能以外のその他の機能を拡張業務機能として区分確定する。

C.3　基本業務機能に係る告知及び明示の同意

基本業務機能に係る告知及び明示の同意の実現方法は、次のとおりである。

a) 基本業務機能の作動前（例：個人情報主体による最初のインストール、初回使用、アカウント登録等）においては、インタラクティブインターフェース

又はインタラクションデザイン（例：ポップアップウィンドウ、文字による説明、入力枠、通知バー、通知音等の形式）を通じて、基本業務機能で収集が必要な個人情報の類型、及び個人情報主体が提供を拒絶し、又は収集への同意を拒絶した場合にもたらされることになる影響を個人情報主体に告知し、かつ、個人情報主体が情報収集に対して自発的に行った肯定的動作（例：「同意する」又は「次へ」へのチェック入力、クリック等）を通じて当該個人情報主体による明示の同意を取得しなければならない。

注：製品又はサービスが提供する基本業務機能について一括で全てを作動させる必要がない場合には、個人情報主体の具体的な使用行為に基づいて基本業務機能を段階的に作動させ、かつ、a)の告知要求を即時完了させることが適当である。

b) 基本業務機能で収集が必要な個人情報の収集に個人情報主体が同意しない場合には、個人情報管理者は、個人情報主体に対する当該業務機能の提供を拒絶することができる。

c) a)で要求されるインタラクティブインターフェース又はインタラクションデザインは、個人情報主体による再アクセス及びその同意範囲の変更に便宜を図るものでなければならない。

注：上記要求の実現方式については、C.5 を参考とすることができる。

C.4　拡張業務機能に係る告知及び明示の同意

拡張業務機能に係る告知及び明示の同意の実現方法は、次のとおりである。

a) 拡張業務機能の初回使用前においては、インタラクティブインターフェース又はインタラクションデザイン（例：ポップアップウィンドウ、文字による説明、入力枠、通知バー、通知音等の形式）を通じて、提供する拡張業務機能及び収集を必要とする個人情報を個人情報主体に逐一告知し、かつ、個人情報主体が拡張業務機能に対し項目ごとに同意選択することを許可しなければならない。

b) 拡張業務機能で収集が必要な個人情報の収集に個人情報主体が同意しない場合には、個人情報管理者は、個人情報主体の同意を繰り返し求めないものとする。個人情報主体が拡張機能の作動を自発的に選択した場合を除き、48 時間内に個人情報主体に対し同意を求める回数は、1 回を超えないものとする。

c) 拡張業務機能で収集が必要な個人情報の収集に個人情報主体が同意しない場合に、基本業務機能の提供を拒絶したり、又は基本業務機能のサービス品質を落としたりしないものとする。

d) a)で要求されるインタラクティブインターフェース又はインタラクションデザインは、個人情報主体による再アクセス及びその同意範囲の変更に便宜を図るものでなければならない。

注：上記要求の実現方式については、C.5 を参考とすることができる。

C.5　インタラクティブ機能インターフェースの設計

個人情報管理者は、表 C.1 に示すテンプレートを参考としてインタラクティブ機能インターフェースを設計し、個人情報主体がその同意選択の権利を十分に行使できるよう保障

することができる。

当該機能インターフェースは、個人情報管理者による個人情報の収集開始前（例：製品インストールの過程、個人情報主体による製品若しくはサービスの初回使用時、又は個人情報主体によるアカウント登録時）において、個人情報管理者が個人情報主体に対し自発的に提供しなければならない。紙媒体資料への記入にて個人情報を収集する場合には、個人情報管理者は、以下のテンプレートの内容を参考として記入用紙をデザインし、もって個人情報主体が同意選択の権利を行使できるよう保障することができる。

表 C.1　インタラクティブ機能インターフェース　テンプレート
（日訳省略）

付属文書 D
（資料性付属文書）
個人情報保護ポリシー　テンプレート
（日訳省略）

表D.1　個人情報保護ポリシー　テンプレート

個人情報保護ポリシー　テンプレート	作成要求
本ポリシーは、XXXXのXXXX製品又はサービス（……を含む。）のみに適用されるものです。 直近更新日：XXXX年XX月 何らかの疑問、ご意見又はご提案がありましたら、以下の連絡先までご連絡をお願いいたします。 Eメール： 電話： ファックス：	（日訳省略）
本ポリシーは、以下の内容についてご理解いただけるようお客様をサポートするものです。 ■ 業務機能1の個人情報収集使用規則 ■ 業務機能2の個人情報収集使用規則 …… ■ 当方がお客様の個人情報をどのように保護するか ■ お客様の権利 ■ 当方がお子様の個人情報をどのように処理するか ■ お客様の個人情報はどのように全世界へ移転されるか ■ 本ポリシーはどのように更新されるか ■ 当方への連絡方法 XXXXは、お客様にとっての個人情報の重要性を心得ており、かつ、全力を尽くしてお客様の個人情報の安全・信頼を守ります。当方は、当方に対するお客様の信用が維持されるよう尽力し、権限・責任一致の原則、目的明確化の原則、同意選択の原則、必要最小限の原則、セキュリティ確保の原則、主体関与の原則、公開透明の原則等の原則を遵守して、お客様の個人情報を保護いたします。XXXXは同時に、業界の確立された安全標準に従って相応の安全保護措置を講じ、お客様の個人情報を保護することを約束いたします。 当方の製品又はサービスを使用される前には、本「個人情報保護ポリシー」を熟読し、かつ、ご理解下さいますようお願い申し上げます。	（日訳省略）

表D.1（続）

個人情報保護ポリシー　テンプレート	作成要求
業務機能1の個人情報収集使用規則 **1、当方がお客様のどのような個人情報を収集するか** ● 当方の提供する業務機能は、部分的な情報に依拠することで運用が可能となります。お客様が当該業務機能の使用を選択される場合には、必要な情報（……を含む合計XX種類の個人情報）について、当方に提供するか、又は当方が収集することを許可していただく必要があります。 ● お客様は、……という合計XX種類の個人情報について、当方に提供するか、又は当方が収集することを許可するかをご自身で選択することができます。これらの情報は、当該業務機能の運用に必須のものではありませんが、サービス品質の改善、新製品又は新サービスの研究開発等にとって非常に重要な意義があるものです。当方は、これらの情報の提供をお客様に強要することはありません。お客様が拒絶されたとしても、当該業務機能の使用に不利な影響が生じることはありません。 ● お客様が当該業務機能を使用される際、当方のアプリは、個人情報に関連する……という合計XX項目のシステム権限をお客様に申請いたします。お客様が授権されない場合、当方が当該業務機能をご提供することは不可能となります。上記の権限の他、お客様は、アプリのその他のシステム権限を追加で付与するか否かをご自身で選択することができます。 **2、当方がお客様の個人情報をどのように使用するか** ● 必要な個人情報について、当方は、当該業務機能（……を含む。）を提供するために使用させていただきます。当方はまた、上記の情報を、本業務機能の維持及び改善、新たな業務機能の開発等に使用いたします。 ● 必要なもの以外の個人情報について、当方は、以下の用途（……を含む。）のために使用させていただきます。 **3、当方がお客様の個人情報をどのように処理委託、共有、譲渡及び公開開示するか** **（1）処理委託** 本業務機能中のある具体的なモジュール又は機能は、外部の供給者から提供されるものです。例えば当方は、サービスプロバイダを招聘してカスタマーサポートの提供に協力させます。 当方が個人情報の処理を委託した会社、組織及び個人に対し、当方は、それらと厳格な秘密保持協定を締結し、当方の要求、本個人情報保護ポリシー並びにその他一切の関連する秘密保持措置及び安全措置に従って個人情報を処理するよう要求い	（日訳省略）

たします。 **（2）共有** 当方は、当社以外のいかなる会社、組織及び個人とも、お客様の個人情報を分け合うことはありません（但し、お客様からの明確な同意を取得した場合を除く。）。現在のところ、当方は以下の場合に、個人情報の共有についてお客様による授権同意を求めます。 a)　…… この場合において現時点で関係する会社、組織及び個人を把握するには、こちらをクリックしてください。【ハイパーリンクを提供】 b)　…… この場合において現時点で関係する会社、組織及び個人を把握するには、こちらをクリックしてください。【ハイパーリンクを提供】 c)　…… この場合において現時点で関係する会社、組織及び個人を把握するには、こちらをクリックしてください。【ハイパーリンクを提供】 当方は、法律法規の規定に基づき、又は政府主管部門の強制的要求に従って、お客様の個人情報を対外的に共有する場合があります。 **（3）譲渡** 当方は、お客様の個人情報を、いかなる会社、組織及び個人にも譲渡することはありません。但し、以下の場合は除きます。 a)　明確な同意を得た場合における譲渡：お客様の明確な同意を得た後、当方は、他の当事者にお客様の個人情報を譲渡いたします。 b)　合併、買収又は破産清算に関係する場合において、個人情報の譲渡に及ぶときは、当方は、この個人情報保護ポリシーによる拘束を引き続き受けるよう、お客様の個人情報を保有する新たな会社・組織に要求いたします。それがなされない場合には、当方は、お客様から新たに授権同意を得るよう当該会社・組織に要求いたします。 **（4）公開開示** 当方は、以下の場合においてのみ、お客様の個人情報を公開開示いたします。 a)　お客様の明確な同意を取得した後 b)　法律に基づく開示：法律、法的手続、訴訟又は政府主管部門による強制的な要求の状況において、当方は、お客様の個人情報を公開開示する場合があります。	

表 D.1（続）

個人情報保護ポリシー　テンプレート	作成要求
業務機能2の個人情報収集使用規則 省略	
当方がお客様の個人情報をどのように保護するか （一）当方は、業界標準に適合する安全防護措置を既に用いてお客様が提供された個人情報を保護しており、授権を経ていないアクセス、公開開示、使用、修正、損壊又は紛失にデータが見舞われることを防止しています。当方は、あらゆる合理的かつ実行可能な措置を講じて、お客様の個人情報を保護いたします。例：?-?- （二）当方は、次の認証を既に取得しています：?-?- （三）当方のデータセキュリティ能力：?-?- （四）当方は、あらゆる合理的かつ実行可能な措置を講じて、無関係の個人情報が収集されないよう確保いたします。当方は、本ポリシー所定の目的の達成に必要な期間内においてのみ、お客様の個人情報を保管いたします（但し、保管期間を延長する必要がある場合又は法律の許可を受けた場合を除く。）。 （五）当方は、セキュリティリスク、個人情報安全影響評価等の報告に関する内容を定期的に更新し、かつ、公開いたします。お客様は、?-?-の方式を通じてこれらを取得することができます。 （六）インターネット環境は、100%安全でありません。当方は、お客様が当方に送信されたあらゆる情報の安全性を確保又は担保することに尽力いたします。当方の物理的、技術的又は管理に係る防護設備が破壊された結果、授権を受けていないアクセス、公開開示、改竄又は破壊に情報が見舞われ、お客様の適法な権益が損害を受けることになった場合には、当方は、相応の法的責任を引き受けます。 （七）遺憾にも個人情報セキュリティインシデントが発生してしまった後には、当方は、法律法規の要求に従い、セキュリティインシデントの基本的な状況及び考えられる影響、当方が既に講じ、又は講じようとしている対処措置、お客様ご自身でリスク防御及びリスク低減が可能となるご提案、お客様に対する救済措置等を、遅滞なくお客様に告知いたします。当方は、インシデントに関連する状況を、メール、信書、電話、プッシュ通知等の方式にてお客様に遅滞なく告知いたします。個人情報主体に逐一告知することが困難である場合には、当方は、合理的かつ有効な方式を講じて公告を掲出いたします。 　同時に、当方は、監督管理部門の要求に従い、個人情報セキュリティインシデントの対処状況についても進んで上級に報告いたします。	（日訳省略）

表D.1（続）

個人情報保護ポリシー　テンプレート	作成要求
お客様の権利 　中国の関連する法律、法規、標準及びその他の国・地域の慣行に従い、当方は、お客様がご自身の個人情報に対し以下の権利を行使することを保障いたします。 **（一）お客様の個人情報へのアクセス** 　お客様には、お客様の個人情報にアクセスする権利があります（但し、法律法規に定められた例外的状況を除く。）。お客様がデータアクセス権の行使をお望みの場合には、……の方式を通じてご自身でアクセスすることができます。 　お客様が上記のリンクを通じてこれらの個人情報にアクセスすることができない場合には、随時当方のWebフォームを使用してご連絡いただくか、又は?-?-宛に電子メールをお送りいただくことができます。 　当方は、30日内にお客様からのアクセス請求に返信いたします。 　お客様が当方の製品又はサービスを使用される過程において生じたその他の個人情報については、当方が過大な資金投入を更に必要としない限り、お客様に提供いたします。お客様がデータアクセス権の行使をお望みの場合には、?-?-宛に電子メールをお送りください。 **（二）お客様の個人情報の訂正** 　当方の処理したお客様に関する個人情報に誤りがあることを発見なさった場合、お客様には、訂正を行うよう当方に要求する権利があります。お客様は、「（一）お客様の個人情報へのアクセス」中にて挙げられた方式を通じて、訂正申請を提出することができます。 　お客様が上記のリンクを通じてこれらの個人情報を訂正することができない場合には、随時当方のWebフォームを使用してご連絡いただくか、又は?-?-宛に電子メールをお送りいただくことができます。 　当方は、30日内にお客様からの訂正請求に返信いたします。 **（三）お客様の個人情報の削除** 　以下の場合において、お客様は、個人情報の削除請求を当方に提出することができます。 1、当方の個人情報処理行為が法律法規に違反する場合 2、当方がお客様の個人情報を収集・使用したが、お客様による同意を取得していなかった場合 3、当方の個人情報処理行為がお客様との約定に違反する場合 4、お客様が当方の製品若しくはサービスの使用をおやめになった場合又はお客様がアカウントを抹消された場合	（日訳省略）

5、当方がお客様に対し製品又はサービスの提供を取りやめた場合 　当方がお客様からの削除請求に対応することを決定した場合には、当方は、当方からお客様の個人情報を取得した実体にも同時に通知し、遅滞なく削除するよう要求いたします（但し、法律法規に別段の定めがある場合又はこれらの実体がお客様の独立した授権を取得している場合を除く。）。 　お客様が当方のサービスから情報を削除した後、当方がバックアップシステムにおいて相応の情報を直ちに削除することはできないかもしれませんが、バックアップ更新時にこれらの情報を削除いたします。 **（四）お客様による授権同意の範囲の変更** 　各業務機能は、いくつかの基本的な個人情報があって初めて完了させることができます。追加的に収集する個人情報の収集及び使用に対し、お客様は、随時ご自身による授権同意を与え、又は撤回することができます。 　お客様は、……の方式を通じご自身で操作することができます。 　お客様が同意を撤回された後、当方が相応の個人情報を更に処理することはありません。但し、お客様による同意撤回の決定が、それ以前にお客様の授権に基づき展開された個人情報の処理に影響することはありません。 　当方がお客様に送信する商業広告の受信を希望されない場合には、お客様は、……の方式を通じて随時取り消すことができます。	

表D.1（続）

個人情報保護ポリシー　テンプレート	作成要求
（五）個人情報主体によるアカウント抹消 お客様は、これまでに登録したアカウントを随時抹消することができ、……の方式を通じご自身で操作することができます。 アカウント抹消後、当方は、お客様への製品又はサービスの提供を停止し、かつ、お客様の要求によりお客様の個人情報を削除いたします（但し、法律法規に別段の定めがある場合を除く。）。 **（六）個人情報主体による個人情報副本の入手** お客様にはお客様の個人情報副本を入手する権利があり、……の方式を通じご自身で操作することができます。 技術的に実行可能であるという前提の下において（例：既にデータインターフェースの整合がとれている。）、当方は、お客様の要求に従い、お客様の個人情報副本をお客様の指定する第三者に直接送信することもできます。 **（七）情報システム自動意思決定の制約** ある業務機能において、当方は、情報システム、アルゴリズム等を含む、人力によらない自動意思決定メカニズムのみによって決定を下す可能性があります。これらの決定がお客様の適法な権益に著しく影響する場合、お客様には当方に説明を要求する権利があり、当方も適当な救済方式を提供いたします。 **（八）お客様からの上記請求への対応** 安全を保障するため、お客様には書面での請求を提供していただくか、又はその他の方式にてお客様の身分を証明していただく必要がある場合がございます。当方は、まずお客様にご自身の身分認証をお願いしてから、お客様の請求を処理することになります。 当方は、30日内に回答を行います。ご納得いただけない場合には、……のルートを通じて苦情を申し立てていただくこともできます。 お客様からの合理的な請求に対し、当方は、原則として費用を徴収いたしません。但し、何度も繰り返される請求や合理的な限度を超えた請求に対しては、当方は、状況に応じて一定のコスト費用を徴収いたします。これらの理由なく繰り返される請求、過大な技術的手段を必要とする（例：新たなシステムの開発又は現行の慣例の根本的な変更を要する）請求、他人の適法な権益にリスクをもたらす請求、又は著しく実情に即していない（例：バックアップテープに保存された情報に関係する）請求に対し、当方は、お断りする場合があります。 以下の場合において、当方は、お客様からの請求に対応する	

ことができません。 1、法律法規に定められた義務の個人情報管理者による履行に関連する場合 2、国家の安全及び国防上の安全に直接関連する場合 3、公共の安全、公衆衛生及び重大な公共の利益に直接関連する場合 4、刑事捜査、提訴、裁判及び判決執行等に直接関連する場合 5、個人情報主体について、主観的悪意の存在又は権利の濫用を示す十分な証拠を個人情報管理者が有する場合 6、個人情報主体又はその他の個人の生命、財産等の重大で適法な権益の維持の為であるにもかかわらず、本人による同意を得ることが困難である場合 7、個人情報主体からの請求に対応することで個人情報主体又はその他の個人・組織の適法な権益が重大な損害を被ることになる場合 　商業秘密に関係する場合	

表D.1（続）

個人情報保護ポリシー　テンプレート	作成要求
当方がお子様の個人情報をどのように処理するか 　当方の製品、ウェブサイト及びサービスは、主として成人を対象としたものです。ご両親又は保護者の方の同意がない場合、お子様がご自身の個人情報主体アカウントを作成されることはありません。 　ご両親の同意を経てお子様の個人情報を収集する状況について、当方は、法律の許可を受けた場合、ご両親若しくは保護者の方が明確に同意する場合又はお子様の保護に必要な場合のみにおいて当該情報を使用又は公開開示いたします。 　地域の法律上及び慣習的に児童の定義が異なったとしても、当方は、14歳未満の全ての方をいずれもお子様とみなします。 　検証可能なご両親の同意を事前に取得しないまま当方がお子様の個人情報を収集したことに当方自身が気付いた場合には、対策を講じて早急に関連データを削除いたします。	
お客様の個人情報はどのように全世界へ移転されるか 　原則として、当方が中華人民共和国国内において収集し、及び生じた個人情報は、中華人民共和国国内において保存されます。 　当方は、全世界に広く分布する資源及びサーバーを通じて製品又はサービスを提供しております。そのため、お客様による授権同意を取得した後、お客様の個人情報は、お客様による製品又はサービスの使用に係る所在国/地域の国外管轄区に移転され、又はこれら管轄区からのアクセスを受ける可能性があるということになります。 　これらの管轄区には異なるデータ保護法が設けられている可能性や、関連法律さえ置かれていない可能性があります。かかる状況下において、当方は、お客様の個人情報が中華人民共和国国内における場合と十分同等な保護を受けるよう確保いたします。例えば当方は、個人情報の越境移転に対するお客様の同意を請求し、又は越境データ移転前においてデータの非識別化等の安全措置を実施いたします。	（日訳省略）

表D.1（続）

個人情報保護ポリシー　テンプレート	作成要求
本ポリシーはどのように更新されるか 　当方の個人情報保護ポリシーは、変更される可能性があります。 　お客様による明確な同意を経ることなく、本個人情報保護ポリシーに従ってお客様が享有すべき権利を当方が削減することはありません。当方は、本ポリシーに対して行ういかなる変更も、本ページ上において発表いたします。 　重大な変更については、当方は、より目立つ通知（あるサービスについて、当方が電子メールを通じて通知を配信し、個人情報保護ポリシーの具体的な変更内容を説明することを含む。）も提供いたします。 　本ポリシーにいう「重大な変更」には以下のものが含まれますが、これらに限られません。 1、当方のサービスモデルに生じた重大な変化（例：個人情報の処理目的、処理される個人情報の類型、個人情報の使用方式等） 2、所有権構造、組織機構等の面で当方に生じた重大な変化（例：事業の見直し、破産・買収等によって引き起こされた所有者の変更等） 3、個人情報の共有、譲渡又は公開開示の主な対象に生じた変化 4、お客様の個人情報処理への関与面での権利及びその行使の方式に生じた重大な変化 5、個人情報安全の処理に責任を負う当方の責任部門、連絡先及び苦情申立てルートに変化が生じた場合 6、個人情報安全影響評価報告によってハイリスクの存在が示された場合 　当方は、本ポリシーの旧バージョンも保存し、お客様の閲覧に供します。	（日訳省略）
当方への連絡方法 　お客様が本個人情報保護ポリシーについて何らかの疑問、ご意見又はご提案をお持ちの場合には、……の方式を通じて当方にご連絡ください。 　当方は、個人情報保護専任部門（又は個人情報保護専任者）を置いています。お客様は、……の方式を通じて当該部門（又は責任者）にご連絡いただくことができます。 　通常の場合、当方は、30日内に返信いたします。 　当方の返信にご満足いただけなかった場合、特に当方の個人情報処理行為がお客様の適法な権益を損なった場合には、お客様は、……の外部ルートを通じて解決案をお求めになることもできます。	（日訳省略）

参考文献

（日訳省略）

（法令原文名称：信息安全技术　个人信息安全规范）