個人情報の安全管理措置に係る基本方針

コムサクシード株式会社

第 1.0 版　令和 6 年 2 月 19 日作成

第１条　はじめに

１．基本方針の目的

①　個人情報の保護と信頼性の確保

組織が取り扱う個人情報の機密性、完全性、可用性を保護し、情報の不正アクセス、紛失、破壊、改ざん、漏洩などのリスクから守ることを目指します。

②　法令遵守

個人情報保護に関連する法律、規則、ガイドライン、及び業界標準などの要求事項を遵守することを確実にします。これには、国内法だけでなく、必要に応じて国際的な法規制も含まれます。

③　リスク管理

個人情報に関連するリスクを特定し、評価した上で、適切なリスク対策を講じることにより、リスクを管理し緩和します。

④　信頼関係の構築

個人情報の適切な管理と保護を通じて、顧客、従業員、ビジネスパートナーなどの関係者との信頼関係を構築し、維持します。

⑤　組織文化の醸成

個人情報保護の重要性についての認識を高め、組織全体で個人情報の安全性を確保するための文化を醸成します。

⑥　透明性の向上

個人情報の収集、利用、管理の方法について透明性を確保し、関係者が個人情報の取り扱いについて理解しやすくすることを目的とします。

⑦　苦情処理と改善

個人情報に関する苦情処理体制を整え、個人情報保護の取り組みを継続的に見直し、改善することを目的とします。

２．適用範囲

①　個人情報の定義

この基本方針が対象とする個人情報の範囲を定義します。これには、氏名、住所、電話番号、メールアドレス、生年月日、性別、職業、勤務先情報、その他個人を識別するための情報が含まれます。

②　処理活動

個人情報の収集、記録、整理、構造化、保管、適応または変更、抽出、参照、利用、開示による伝達、普及またはその他の形での提供、照合またはリンク、制限、消去または破棄など、個人情報に関連するすべての処理活動をカバーします。

③　物理的及び電子的な情報

紙の文書及び電子的なデータ両方に適用されることを明確にします。

④　地理的範囲

組織の運営地域内外で処理される個人情報にも適用されることを示します。また、国際的なデータ転送に関する特別な考慮事項が含まれる場合があります。

3．対象者

① 従業員

全ての従業員、包括的には正社員、契約社員、パートタイム社員、一時雇用者、インターン等が含まれます。

② 協力会社及び外部パートナー

組織と個人情報を共有する協力会社、ベンダー、サプライヤー、顧問などの外部パートナーが含まれます。

③ 顧客

組織の提供する商品やサービスの利用者、およびその見込み客が含まれます。

④ その他の関係者

個人情報を提供する可能性のあるその他の関係者、例えばウェブサイトの訪問者や調査参加者等

第２条　個人情報の管理体制

① 組織内の個人情報保護責任者

管理者名：田中　正人

連絡先：メールアドレス：privacy@comsucceed.jp

② 役割と責任

1. ポリシーの策定と実施

個人情報保護方針の策定、更新、および実施を監督します。

2. コンプライアンスの監視

個人情報の取り扱いが法令、規則、及び組織のポリシーに準拠していることを監視します。

3. リスク管理

個人情報に関連するリスクを評価し、リスク軽減策を提案します。

4. 教育と訓練

従業員に対して個人情報保護の重要性について教育し、適切な訓練を提供します。

5. 監査とレポート

定期的な個人情報保護の監査を実施し、経営層に対してレポートします。

6. 関係者とのコミュニケーション

個人情報の主体や規制当局とのコミュニケーション窓口となります。

7. インシデント対応

データ漏洩やセキュリティ違反が発生した場合の対応計画を立案し、実施します。

第３条　個人情報の収集、利用、提供

① 個人情報の収集に関する基準

1. 合法性、公正性、透明性

個人情報は、法律に基づき、公正かつ透明な方法で収集する必要があります。関係者は、自分の情報がどのように、なぜ収集されるのかを理解できるように情報提供を行います。

2. 目的の特定と限定

収集する個人情報の目的を明確に特定し、記録する必要があります。情報は、特定された目的のためにのみ使用されます。

3. データの最小化

必要な目的を達成するために必要な限りの個人情報のみを収集するべきです。過剰なデータ収集は避け、収集したデータは目的に関連し、適切で、限定されます。

4. 正確性

収集した個人情報は正確であり、必要に応じて最新の状態に保たれ、不正確なデータは、発見次第、速やかに訂正または削除します。

5. 保存期間の限定

個人情報は、特定の目的を達成するために必要な期間のみ保持され。その期間が終了したら、情報は安全に削除または匿名化されます。

6. データの安全性

収集した個人情報は、不正アクセス、紛失、破壊、改ざん、漏洩などから保護するための適切なセキュリティ措置によって保護されます。

7. 個人の権利の尊重

情報の主体は、自己の個人情報に関する権利（アクセス権、訂正権、削除権、データの移動性の権利など）を行使します。

8. 責任とアカウンタビリティ

組織は、これらの原則に従って個人情報を収集し、管理する責任を負います。また、要求に応じてその遵守を証明することが求められる場合があります。

② 個人情報の利用目的の特定及び遵守

1. 利用目的の明確化

・特定

収集する個人情報が何のために使われるかを明確にし、具体的に特定します。
この目的は、合法的、公正、かつ透明なものでなければなりません。

・文書化

利用目的を文書化し、情報主体がアクセス可能な形式で公開します。これにより、透明性が確保されます。

2. 利用目的の通知

・情報主体への通知

個人情報を収集する際、事前にその目的を情報主体に通知します。通知には、収集

される情報の種類、利用目的、共有される可能性がある第三者についての情報が含まれます。

・同意の取得

特定のケースでは、情報主体の明示的な同意が必要になる場合があります。同意は、自由かつ情報に基づいたものでなければなりません。

3. 利用目的の限定

・目的限定の原則

収集した個人情報は、事前に特定した目的のためにのみ使用され、目的外の利用は、原則として許可されません。

・変更時の手続き

利用目的を後から変更する必要が生じた場合、改めて情報主体の同意を得るか、適切な法的根拠が必要になります。

4. 遵守と監視

・内部ポリシーと手順

組織は、個人情報の利用目的を遵守するための内部ポリシーと手順を設け、これを従業員に周知徹底させます。

・定期的なレビュー

利用目的の遵守状況を定期的にレビューし、監査します。これにより、透明性とアカウンタビリティが確保されます。

5. 情報主体の権利の尊重

・権利の保護

情報主体は、自己の個人情報に関するアクセス権、訂正権、削除権、利用制限権、データ移動権などの権利を行使することができます。

・権利行使の支援

組織は、これらの権利を行使するための手続きを簡易かつアクセスしやすい形で提供する必要があります。

③ 個人情報の第三者提供の制限と手続

1. 制限

・法的根拠

個人情報を第三者に提供する前に、適切な法的根拠が存在することを確認します。これには、情報主体の同意が必要な場合や法律により許可されている場合が含まれます。

・情報主体の同意

特定の状況では、情報主体の明示的な同意を取得する必要があります。同意は、自由かつ情報に基づいている必要があり、情報主体はいつでも撤回することができます。

・最小限の情報提供

必要最小限の個人情報のみを提供し、提供する情報の範囲を限定します。目的に不必要な情報は提供しないようにします。

2. 手続き

・契約及び合意書

第三者との間で、個人情報の保護に関する契約または合意書を締結します。これには、データ保護の義務、データの使用目的、安全管理措置、データ違反時の通知義務などが含まれます。

・情報主体への通知

個人情報を第三者に提供すること、提供される情報の範囲、提供の目的、および情報主体が自己の情報に関して持つ権利について情報主体に通知します。

・第三者の選定と監査

個人情報を取り扱う第三者の選定には注意を払い、定期的にそのデータ保護の実践とポリシーを監査します。

・安全管理措置の確認

第三者が適切な安全管理措置を講じていることを確認します。これには、物理的、技術的、組織的措置が含まれます。

3. 透明性とアカウンタビリティ

・データ保護影響評価

特定のリスクが伴う提供の場合、データ保護影響評価を実施する場合があります。

・記録の保持

個人情報の第三者提供に関する記録を保持し、必要に応じて規制当局や情報主体に対してこれらの記録を提供できるようにします。

第４条　安全管理措置

① 技術的安全管理措置（アクセス制御、暗号化など）

１．制限

・法的根拠

個人情報を第三者に提供する前に、適切な法的根拠が存在することを確認します。これには、情報主体の同意が必要な場合や法律により許可されている場合が含まれます。

・情報主体の同意

特定の状況では、情報主体の明示的な同意を取得する必要があります。同意は、自由かつ情報に基づいている必要があり、情報主体はいつでも撤回することができます。

・最小限の情報提供

必要最小限の個人情報のみを提供し、提供する情報の範囲を限定します。目的に不

必要な情報は提供しないようにします。

2．手続き

・契約及び合意書

第三者との間で、個人情報の保護に関する契約または合意書を締結します。これには、データ保護の義務、データの使用目的、安全管理措置、データ違反時の通知義務などが含まれます。

・情報主体への通知

個人情報を第三者に提供すること、提供される情報の範囲、提供の目的、および情報主体が自己の情報に関して持つ権利について情報主体に通知します。

・第三者の選定と監査

個人情報を取り扱う第三者の選定には注意を払い、定期的にそのデータ保護の実践とポリシーを監査します。

・安全管理措置の確認

第三者が適切な安全管理措置を講じていることを確認します。これには、物理的、技術的、組織的措置が含まれます。

② 物理的安全管理措置（施設のセキュリティ、文書の保管方法など）

1．施設のセキュリティ

・アクセス制御

不正アクセスを防ぐために、物理的な入出口の管理を強化します。セキュリティゲート、ガード、アクセスカードシステム、顔認証や指紋認証などの生体認証システムを導入します。

2．文書の保管方法

・ロック可能な保管設備

紙の文書や記録が含まれるファイルキャビネットや保管室は、適切にロックして不正アクセスを防ぎます。

・アクセス管理

重要な文書にアクセスできる人員を限定し、アクセスリストを管理します。文書へのアクセスは、必要な業務に直接関連する人員に限定されます。

・廃棄プロトコル

個人情報が含まれる文書の廃棄時には、シュレッダーで細断するなど、情報が復元不可能な状態になるよう適切な処理を行います。

3．施設のセキュリティ

③ 組織的安全管理措置（社内規程の整備、従業員への教育訓練など）

1．社内規程の整備

・個人情報保護ポリシーの策定

組織の個人情報保護に関する基本方針、目的、責任者、および手続きを明確に記述

した文書を作成します。

・アクセスポリシー

個人情報へのアクセス権を持つ従業員を限定し、その基準と手続きを定めます。

・データ分類と取り扱い規程

情報を機密性の度合いに応じて分類し、各カテゴリーの情報に適用される保護措置を規定します。

2．従業員への教育訓練

・定期的な教育プログラム

個人情報保護の重要性と、従業員の責任についての認識を高めるために、定期的な教育訓練を実施します。

・新入社員研修

新入社員に対して、個人情報保護に関する基本的な知識と組織のポリシーを理解させるための研修を提供します。

・特定の役割向けの専門トレーニング

個人情報の取り扱いに直接関わる従業員に対して、その役割に特化した専門的なトレーニングを提供します。

3．監査と監視

・定期的な自己監査

個人情報保護の実践とポリシーの遵守状況を確認するための内部監査を定期的に実施します。

・外部監査

必要に応じて、第三者機関による外部監査を受け、個人情報管理体制の有効性を評価します。

4．インシデント管理と対応

・インシデント対応計画

データ漏洩やセキュリティ違反が発生した場合の対応プロセスを定め、迅速かつ効果的な対応を可能にします。

・定期的な演習

インシデント対応計画の効果を確認し、改善点を見つけるために、定期的な演習を実施します。

5．コミュニケーションと意識向上

・内部コミュニケーション

個人情報保護に関する最新の情報、ガイドラインの更新、重要な通知などを定期的に従業員に伝えます。

第5条　個人情報の正確性と安全性の確保

①　個人情報の正確性を確保するための措置

1．収集時の正確性確保

・情報源の確認

収集する個人情報が信頼できる情報源から得られることを確認します。

・直接収集の原則

可能な限り、情報主体から直接個人情報を収集し、その際に情報の正確性を確認します。

2．情報主体による確認と訂正

・アクセスと訂正の権利

情報主体が自己の個人情報にアクセスし、不正確な情報を訂正または削除する権利を持つことを保証します。

・簡易な手続き

情報主体が自己の情報にアクセスし、必要に応じて更新または訂正できるよう、簡単かつ迅速に手続きを行える仕組みを提供します。

3．定期的なレビューと更新

・情報の定期的なレビュー

個人情報が時代遅れにならないように、定期的に情報のレビューと更新を行います。

・データ品質の監査

個人情報の品質と正確性を保証するための内部監査を定期的に実施します。

4，データ整合性の維持

・データ整合性のチェック

データベース内の個人情報の整合性を確保するために、定期的なチェックを行い、矛盾や重複がないかを監視します。

・エラー検出と修正プロセス

データ入力や転送の過程で発生する可能性のあるエラーを検出し、迅速に修正するプロセスを確立します。

5，技術的措置の利用

・バリデーションツール

データ入力時に形式や内容の正確性を確認するためのバリデーションツールやソフトウェアを利用します。

・データクレンジングツール

不正確または不完全なデータを識別し、修正または削除するためのデータクレンジングツールを使用します。

6．従業員の教育と意識向上

・個人情報の取り扱いに関する教育

従業員に対し、個人情報の正確性を維持する重要性と、そのための適切な手順につ

いて定期的な教育を提供します。

・意識向上プログラム

個人情報の正確性を維持するためのベストプラクティスやガイドラインを共有し、従業員の意識向上を図ります。

② リスク管理と漏洩防止策

1．リスク評価と分析

・リスクアセスメントの実施

定期的にリスクアセスメントを実施し、個人情報を取り巻く脅威と脆弱性を特定します。

・影響分析

リスクが実現した場合の組織や情報主体に対する影響を評価します。

2．データ保護ポリシーの策定と実施

・データ保護ポリシー

個人情報の取り扱いに関する明確なポリシーを策定し、全従業員に周知します。

情報を分類し、機密性の高いデータにはより厳格な保護措置を適用します。

・アクセス制御とユーザー管理

最小限の権限原則

従業員には、その業務遂行に必要な情報へのアクセス権のみを付与します。

アクセスログの監視と分析

不正アクセスの試みや不審な行動を検出するために、アクセスログを定期的に監視し分析します。

3．物理的および技術的セキュリティ措置

・暗号化

転送中および保存中のデータを暗号化します。

・セキュリティソフトウェアの更新

ウイルス対策ソフトウェアやその他のセキュリティソフトウェアを最新の状態に保ちます。

4．従業員の教育と意識向上

・定期的なセキュリティ教育

従業員に対して、個人情報保護とセキュリティ意識に関する定期的な教育を提供します。

・フィッシング対策トレーニング

フィッシング攻撃やその他の社会工学的攻撃に対する警戒心を高めるためのトレーニングを実施します。

5．インシデント対応計画

・インシデント対応計画の策定

データ漏洩やセキュリティ違反が発生した場合の対応計画を策定し、事前に準備します。

・迅速な対応と通知

インシデント発生時には迅速に対応し、必要に応じて関係当局や影響を受けた情報主体に通知します。

6．事後分析と改善

・事後分析

セキュリティインシデント後には、原因を分析し、再発防止のための改善策を実施します。

・継続的な改善プロセス

リスク管理プロセスとセキュリティ対策を継続的に見直し、改善します。

第6条　監視と見直し

①　定期的な監査と評価

・監査の範囲の定義

監査の範囲を明確に定義し、個人情報の収集、処理、保管、送信などのすべての関連するプロセスを対象にします。

・監査の計画とスケジューリング

定期的な監査のスケジュールを設定し、監査計画を策定します。これには、監査の目的、範囲、リソース、実行スケジュールなどが含まれます。

・監査の実施

監査を実施するために、内部の専門家や外部の専門家によるチームを組織し、監査手順を遵守します。これには、文書レビュー、システムアクセスの評価、インタビュー、物理的なセキュリティの評価などが含まれます。

・評価と報告

監査結果を評価し、特定のリスクや問題点を特定します。監査報告書には、発見された問題、改善すべきポイント、提案された対策などが含まれます。

・対策の実施と改善

監査報告書に基づいて、個人情報の安全管理に関連する問題を解決するための対策を実施します。これには、ポリシーや手順の改善、セキュリティの強化、従業員のトレーニングなどが含まれます。

・フィードバックと監査のサイクルの継続

実施された対策の効果を評価し、フィードバックを受け取ります。これにより、個人情報の安全管理のプロセスが継続的に改善されます。

②　改善措置と方針の見直し

1．改善措置のプロセス

・問題点の特定

監査、インシデントの報告、またはリスク評価を通じて、セキュリティの弱点や遵守の不備を特定します。

・原因分析

特定された問題の根本原因を分析します。これには、プロセスの不備、技術的欠陥、または従業員の意識の欠如が含まれる場合があります。

・改善策の策定

根本原因を解決するための具体的な改善策を策定します。これには、プロセスの改善、技術的なセキュリティ対策の強化、または教育・訓練プログラムの導入が含まれる場合があります。

・実施計画の作成

改善策を実施するための詳細な計画を作成し、責任者、タイムライン、必要なリソースを明確にします。

・改善策の実施

計画に従って改善策を実施します。実施過程で発生する可能性のある問題に対処するための準備も重要です。

・効果の評価とモニタリング

改善策の効果を評価し、目標が達成されたかどうかをモニタリングします。必要に応じて追加の改善策を実施します。

２．方針の見直しプロセス

・現行方針の評価

現在の個人情報保護方針の有効性を評価し、遵守状況を確認します。

・環境の変化の評価

法規制、技術、業界基準、および組織内の変化を考慮し、これらが個人情報保護方針に与える影響を評価します。

・ステークホルダーのフィードバックの収集

従業員、顧客、およびその他の関係者からのフィードバックを収集し、方針の改善に役立てます。

・改訂案の策定

必要に応じて方針の改訂案を策定し、関連するステークホルダーにレビューを依頼します。

・改訂方針の承認と公表

改訂案を最終承認し、方針の変更を組織内外に公表します。

・実施と教育

改訂された方針を実施し、関連する従業員に対して必要な教育や訓練を提供します。

第７条　苦情処理及び相談窓口

① 個人情報に関する苦情処理の体制

コムサクシード株式会社　個人情報問合せ窓口

〒101-0031　東京都千代田区岩本町３－１１－８　イワモトチョービル４１４

メールアドレス：privacy@comsucceed.jp　TEL：03-5823-7380

（受付時間　09:00～18:00※土・日曜日、祝日、年末年始、ゴールデンウィークを除く）

第８条　法令及び規範の遵守

①　関連する法令、規範、ガイドラインの遵守（参考）

１．個人情報の保護に関する法律（個人情報保護法）

日本の個人情報保護法は、個人情報の取り扱いに関する基本的な法律です。この法律は、個人情報を取り扱う事業者に対して、適切な取得、利用、提供、安全管理などの義務を課しています。また、個人情報の取り扱いに関して適用される基準や、個人の権利を保護するための措置が定められています。

２．特定個人情報の保護に関する法律（マイナンバー法）

特定個人情報（マイナンバー）の取り扱いに関して、個人情報保護法よりも厳格な規制を設ける法律です。特定個人情報の適切な取り扱いや、安全管理措置の義務付け、違反した場合の罰則などが定められています。

３．情報セキュリティ管理基準

日本では、情報セキュリティの管理に関して、JIS Q 27001（ISO/IEC 27001 に相当）などの国際規格に基づく管理基準が採用されています。これにより、情報セキュリティのリスク管理、物理的・技術的安全対策、組織的なセキュリティポリシーの策定などが推奨されています。

４．ガイドラインおよび業界団体の規則:

個人情報保護委員会などの政府機関や、経済産業省、総務省などが発行するガイドラインも重要です。これらのガイドラインは、法律の具体的な適用方法や、特定の業界における個人情報の取り扱い方について詳細な指示を提供しています。

また、情報サービス産業や電子商取引など特定の分野における業界団体が独自の規則やガイドラインを設け、その業界内での個人情報の取り扱い基準を高めています。

第９条　終わりに

① 基本方針の重要性と従業員の責任

１．個人情報の基本方針の重要性

信頼の構築

個人情報の適切な取り扱いを公にすることで、顧客や取引先からの信頼を獲得し、ビジネスの基盤を強化します。

法令遵守

個人情報保護法やマイナンバー法など、遵守すべき法令が多岐にわたります。基本方針を持つことで、これらの法令や規範への準拠を組織全体で徹底できます。

リスク管理

情報漏洩や不正アクセスなどのリスクから個人情報を守るための体系的な対策を定めることができます。これにより、セキュリティインシデント発生時の対応策や、その影響を最小限に抑えることが可能になります。

内部統制の強化

個人情報の取り扱いに関する基本方針やプロセスを明確にすることで、従業員の行動基準を統一し、内部統制を強化します。

２．従業員の責任

法令・方針の理解と遵守

従業員は、個人情報保護に関連する法令や企業の基本方針を正確に理解し、日常業務において遵守する責任があります。

定期的な研修への参加

個人情報保護に関する知識は常に更新されています。従業員は、定期的な研修や教育プログラムに参加し、最新の情報を習得することが求められます。

セキュリティ対策の実施

パスワード管理、アクセス権限の適切な管理、不正アクセスやウイルスからの保護措置など、個人情報を保護するためのセキュリティ対策を適切に実施する責任があります。

違反時の報告

個人情報の不正な取り扱いを発見した場合や、セキュリティインシデントが発生した場合は、直ちに報告するシステムが整えられており、従業員はこれに従う責任があります。

② 改訂歴及び文書管理

第 1.0 版　令和６年２月１９日作成