総務省 安心してインターネットを使うために

国民のためのサイバーセキュリティサイト

組織幹部のための情報セキュリティ対策

企業や組織にとって、情報セキュリティ対策は、いまや重要な経営課題のひとつです。

情報セキュリティ対策には、組織全体の基本方針の策定や、適切な投資が必要であり、組織幹部の意志決定が欠かせません。組織幹部には、自分たちの組織にはどのような情報資産があり、どのようなリスクがあるかを把握した上で、自ら率先して情報セキュリティ対策の指揮を執ることが求められます。

ここでは、組織幹部のための情報セキュリティ対策として、情報セキュリティ対策の必要性、情報セキュリティマネジメントの考え方、個人情報を取り扱う企業としての責務などについて説明します。

なお、組織幹部自身が、実際にコンピュータやインターネットを利用する際に必要な対策は、「社員・職員全般の情報セキュリティ対策」を参照してください。

組織幹部のための情報セキュリティ対策

情報セキュリティ対策の必要性

いまや情報システムやインターネットは、企業や組織の運営に欠かせないものになりました。しかし、現在の企業や組織は、情報システムへの依存による利便性の向上と引き換えに、大きな危険性を抱え持つことになってしまいました。情報システムの停止による損失、顧客情報の漏洩（ろうえい）による企業や組織のブランドイメージの失墜など、情報セキュリティ上のリスクは、企業や組織に大きな被害や影響をもたらします。また、多くの場合、被害や影響は取引先や顧客などの関係者へも波及します。

企業や組織にとって、情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつと考えなければなりません。特に、個人情報や顧客情報などの重要情報を取り扱う場合には、これを保護することは、企業や組織にとっての社会的責務でもあります。

今日、情報セキュリティ対策は、世界的にも重要な経営課題であると認識されており、情報セキュリティ製品・システム評価基準（ISO/IEC15408）や情報セキュリティマネジメントシステムの認証基準（ISO/IEC27001）が、国際標準として規格化されています。情報セキュリティ対策の重要度が高まるにつれて、日本国内においても、これらの国際基準を採用する企業が増えてきています。

ここでは、企業における情報セキュリティに係る主要な事故やトラブルとその影響を紹介します。

■ 機密情報の漏洩

機密情報の漏洩は企業・組織の競争力や信頼を大きく損なう可能性があります。ウイルスへの感染や社員による不正な情報の持ち出し、あるいは記録媒体の紛失など、さまざまな原因により、多くの組織で情報漏洩が実際に発生しています。

■ 個人情報の流出

保有する個人情報を流出させてしまった場合、賠償や訴訟などの大きな問題にまで発展することがあります。また、企業のブランドイメージを大きく低下させ、顧客離れなど、経営に大きな影響が出る可能性があります。

■ ホームページの改ざん

インターネットでの企業の顔とも言えるホームページが改ざんされるということは、企業イメージの損失につながります。さらに、ウイルスを埋め込まれてしまった場合には、ホームページの訪問者のコンピュータを感染させてしまうこともあります。

これらのことは、会社としての情報セキュリティ対策が不足しているということを露呈することにもなり、取引会社からの信頼を失い、取引停止などにつながるかもしれません。

■ システムの停止

社内の基幹システムが停止してしまうと、最悪の場合、業務自体が停止してしまうこともあります。その間に顧客が競合会社のサービスに移動してしまい、販売機会を失うことになるかもしれません。

■ ウイルスへの感染

ウイルス感染は、上で述べたようなさまざまなトラブルの原因になります。その他、ウイルスは、既に感染したパソコンを使って、ウイルス自身を複製して他のパソコンに感染を広げたり、利用者が気づかないところでネットワーク上の他のパソコンを攻撃したりすることがあります。組織としてこうした情報セキュリティ対策の不十分なパソコンを保有することで、結果的に他者に損害を与えてしまい、社会的な非難や、損害賠償請求を受ける可能性もあります。

企業や組織の幹部は、こういったリスクが、組織の規模に関係なくどのような組織にも存在していることを認識し、これらのリスクを可能な限り軽減するために、組織に適切な情報セキュリティ対策を導入する必要があります。

情報セキュリティの概念

企業や組織における情報セキュリティとは、企業や組織の情報資産を「機密性」、「完全性」、「可用性」に関する脅威から保護することです。

情報資産とは、企業や組織などで保有している情報全般のことです。顧客情報や販売情報などの情報自体に加えて、それらを記載したファイルや電子メールなどのデータ、データが保存されているパソコンやサーバなどのコンピュータ、CD-ROMやUSBメモリ、SDカードなどの記録媒体、そして紙の資料も情報資産に含まれます。

- 機密性

  機密性（Confidentiality）とは、許可された者だけが情報にアクセスできるようにすることです。許可されていない利用者は、コンピュータやデータベースにアクセスすることができないようにしたり、データを閲覧することはできるが書き換えることはできないようにしたりします。

- 完全性

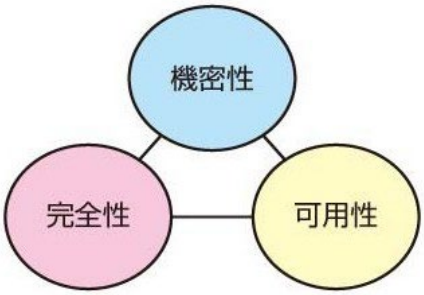
  完全性（Integrity）とは、保有する情報が正確であり、完全である状態を保持することです。情報が不正に改ざんされたり、破壊されたりしないことを指します。

- 可用性

  可用性（Availability）とは、許可された者が必要なときにいつでも情報にアクセスできるようにすることです。つまり、可用性を維持するということは、情報を提供するサービスが常に動作するということを表します。

情報資産を脅かす具体的な脅威として、機密情報の漏洩（ろうえい）や不正アクセス、データの改ざん、サービスの停止などが挙げられます。

企業や組織においては、保有する情報資産の特質をよく検討して、機密性、完全性、可用性のバランスを考慮しながら情報セキュリティ対策を行うことが大切です。



必要な情報セキュリティ対策

組織や企業を脅かす情報セキュリティ上のリスクにはさまざまなものがあり、必要な情報セキュリティ対策も多様です。

例えば、組織や企業で発生する可能性のあるトラブルとそれぞれの情報セキュリティ対策には、以下のようなものがあります。

これらの多様なリスクに対して、実際の被害が発生する前に必要な対策を講じておくためには、また、組織の限られたリソースで最大限の効果を上げるためには、どうしたら良いのでしょうか。

まずは、組織としてあらかじめ情報セキュリティ対策の方針と規則を定めることが必要です。このような、規定化された情報セキュリティ対策の方針や行動指針を情報セキュリティポリシーと言います。

そして、すべての社員や職員に情報セキュリティに関する教育を行い、情報セキュリティポリシーに沿った行動が実行されるよう、意識の向上を促すことが必要です。組織の実態や社会の変化に合わせた定期的な情報セキュリティポリシーの見直しも必要です。こうした情報セキュリティポリシーの策定から実際の運用・改善までを含めた活動全体を、情報セキュリティマネジメントといいます。

企業や組織においては、組織幹部の指揮のもと、情報セキュリティマネジメントを確実に実行していくことが必要です。

情報セキュリティマネジメントとは

企業・組織における情報セキュリティの確保に組織的・体系的に取り組むことを情報セキュリティマネジメントといいます。ここでは、その実施サイクルと、対策の中心となる情報セキュリティポリシーの策定・運用・改善手順について説明します。

- 情報セキュリティマネジメントの実施サイクル
- 情報セキュリティポリシーの概要と目的
- 情報セキュリティポリシーの内容
- 情報セキュリティポリシーの策定
- 情報セキュリティ教育の実施
- 情報セキュリティポリシーの評価と見直し
- 事故やトラブル発生時の対応

情報セキュリティマネジメントの実施サイクル

情報セキュリティマネジメントを実施するにあたっては、まず計画段階として、情報セキュリティポリシーを策定します。しかし、情報セキュリティポリシーは、一度文書化して策定するだけではあまり効果が期待できません。以下のような情報セキュリティマネジメントの実施サイクル(PDCAサイクル)によって、実態に沿った内容になっているかを常にチェックし、絶えず見直し、改善を図ることが大切です。

計画(Plan):

情報資産の洗い出しを行い、リスクや課題を整理し、組織や企業の状況に合った情報セキュリティ対策の方針を定めた情報セキュリティポリシーを策定する。

導入・運用(Do):

全社員・全職員に周知し、必要に応じて、集合研修などの教育を行う。社員・職員が情報セキュリティポリシーに則って行動することで、目的とする情報セキュリティレベルの維持を目指す。

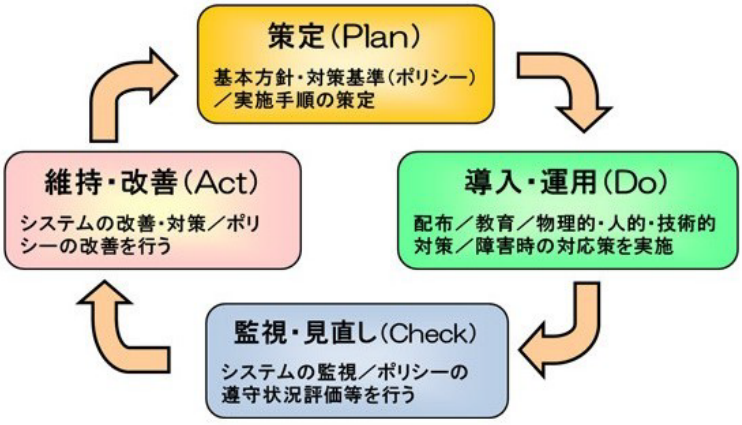
点検・評価(Check):

導入後の現場の状況や問題点、社会的な状況などを踏まえて、定期的に情報セキュリティポリシー自体を評価する。また、遵守されているかどうかの監査も行う。

見直し・改善(Act):

点検・評価の内容を参考にして、情報セキュリティポリシーの見直し・改善を行う。

情報セキュリティポリシーは、企業や組織の状況、新たな脅威、新しい法律の施行など社会的な状況によっても、定期的に見直さなければなりません。そのためにも、このようなサイクルを継続的に実施することで、常に適切なものにしておくことが大切です。



情報セキュリティポリシーの概要と目的

情報セキュリティポリシーとは、企業や組織において実施する情報セキュリティ対策の方針や行動指針のことです。情報セキュリティポリシーには、社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的です。

情報セキュリティ対策は画一的なものではなく、企業や組織の持つ情報や組織の規模、体制によって、大きく異なります。つまり、業務形態、ネットワークやシステムの構成、保有する情報資産などを踏まえた上で、その内容に見合った情報セキュリティポリシーを作成しなければなりません。

情報セキュリティポリシーを作成する目的は、企業の情報資産を情報セキュリティの脅威から守ることですが、その導入や運用を通して社員や職員の情報セキュリティに対する意識の向上や、取引先や顧客からの信頼性の向上といった二次的なメリットを得ることもできます。

情報セキュリティポリシーを整備する上で大切なことは、情報セキュリティ担当者だけがネットワークやパソコンなどに対する情報セキュリティ対策を心がければよいというものではないという点です。情報資産を共有するすべての社員や職員が適切な情報セキュリティ意識を持たなければ、ウイルス、情報漏洩（ろうえい）などから組織を防御することは困難です。

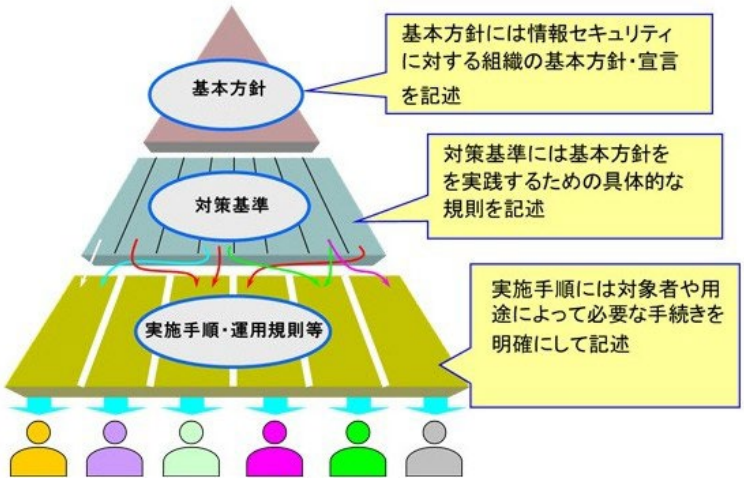
情報セキュリティポリシーの内容

情報セキュリティポリシーは、「基本方針」、「対策基準」、「実施手順」の三つの階層で構成されることが一般的です。

基本方針には、組織や企業の代表者による「なぜ情報セキュリティが必要であるのか」や「どのような方針で情報セキュリティを考えるのか」、「顧客情報はどのような方針で取り扱うのか」といった宣言が含まれます。

対策基準には、実際に情報セキュリティ対策の指針を記述します。多くの場合、対策基準にはどのような対策を行うのかという一般的な規定のみを記述します。

実施手順には、それぞれの対策基準ごとに、実施すべき情報セキュリティ対策の内容を具体的に手順として記載します。



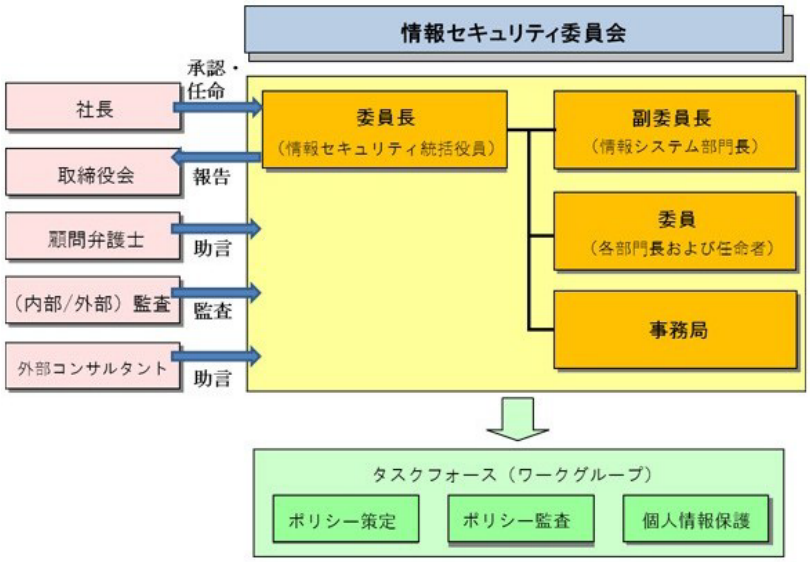
情報セキュリティポリシーの策定

情報セキュリティポリシーを策定する際にもっとも大切なことは、担当者、体制、手順をあらかじめ検討しておくということです。また、情報セキュリティポリシーは、企業や組織の代表者が施行するものであるため、可能な限り、代表者や幹部が策定の作業自体にも関わるような体制を作ることが重要です。

策定のための体制作り

情報セキュリティポリシーを策定し運用するには、まず責任者を明確にして、情報セキュリティポリシー策定に携わる人材を組織化することが必要になります。この組織の活動内容が情報セキュリティポリシー策定・運用の成果に大きく影響するため、企業や組織の実情や現在の社会状況に見合った情報セキュリティポリシーを策定・運用するためには、適切な人材を確保する必要があります。また、情報セキュリティポリシーの品質を高めるためには、外部のコンサルタントや法律の専門家に参加を依頼することも検討するとよいでしょう。

ただし、外部のコンサルタントに策定の全てを依頼することはふさわしくありません。これは、組織内の者によって情報セキュリティポリシーを策定しなければ、その企業や組織に適した内容にすることが困難であるためです。できるだけアドバイザなどの形で協力してもらうようにしましょう。



策定の手順

情報セキュリティポリシーの策定手順は、業態、組織規模、目的、予算、期間などによって大きく異なります。ここでは、代表的な策定手順を紹介します。

1. 策定の組織決定（責任者、担当者の選出）
2. 目的、情報資産の対象範囲、期間、役割分担などの決定
3. 策定スケジュールの決定

4. 基本方針の策定
5. 情報資産の洗い出し、リスク分析とその対策
6. 対策基準と実施内容の策定

策定時の留意事項

効果的な情報セキュリティポリシーを策定するには、以下の点に留意する必要があります。

- 守るべき情報資産を明確にする。
- 対象者の範囲を明確にする。
- できる限り具体的に記述する。
- 社内の状況を踏まえて、実現可能な内容にする。
- 運用や維持体制を考慮しながら策定する。
- 形骸化を避けるために、違反時の罰則を明記する。

基本方針

ポリシーの目的
ポリシーの適用範囲
ポリシーの適用対象者
体制及び構成と役割
ポリシー文書構成
ポリシー監査
ポリシー違反発見時の対応
……

対策基準	実施手順
入退出の管理基準	入退出管理マニュアル
施設内における管理	IDカード発行手順
セキュリティ教育基準	訓練手順・E-ラーニング実施手順
コンピュータウィルス対策基準	ウイルス対策ソフト導入手順
社内ネットワーク利用基準	クライアントのネットワーク設定マニュアル

情報セキュリティ教育の実施

策定した情報セキュリティポリシーに関しては、組織幹部も含め全社員や職員に情報セキュリティ教育を実施して、遵守することを徹底しなければなりません。

単に、分厚い資料を渡したり、形だけの方針や指針を伝えたりするだけでは、社員や職員に情報セキュリティポリシーに則って行動してもらうことはできません。

そのため、情報セキュリティに関する同意書にサインしてもらう、違反時の規定を設けるなどの方法で、情報セキュリティポリシーを意識させる仕組みが必要です。また、情報セキュリティ診断システムなどを利用して、導入した情報セキュリティ対策の効果や情報セキュリティポリシーの浸透具合をチェックするというのも効果的です。

また、インシデント発生を想定した演習を定期的に行うことも有効です。この演習は、情報セキュリティ担当部署のみが実施すればよいものではなく、組織幹部から一般社員まであらゆる立場の社員・職員の参加が望ましいです。

全ての社員や職員が遵守するからこそ、情報セキュリティポリシーに意味があり、情報セキュリティ対策が効果的になります。そのような情報セキュリティに対する意識を社員や職員一人一人に啓発することが、企業や組織における大切な情報セキュリティ対策のひとつです。

情報セキュリティポリシーの評価と見直し

情報セキュリティポリシーは、運用を開始した後にも、社員や職員の要求や社会状況の変化、新たな脅威の発生などに応じて、定期的な見直しが必要です。また、見直しを行った結果、必要に応じて情報セキュリティポリシーを改訂しなければなりません。この作業を継続的に繰り返すことが、情報セキュリティ対策の向上に役立ちます。

情報収集、評価、監査、リスク分析

情報セキュリティ上のリスクは、常に変化しているものです。情報セキュリティ対策もその変化に対応できなければなりません。そのため、常に最新の情報セキュリティ関連の情報を収集する体制が必要です。そして、収集した情報を参考にして、現在の情報セキュリティポリシーの内容に不足している項目がないかどうかを評価します。

評価のためには、日常的に社員や職員へのモニタリングを行い、情報セキュリティポリシーが適切に守られているか、有効に機能しているかなどについての調査、定期的な監査、変動するリスクの分析などを行います。

評価をする際には、情報セキュリティポリシーが現場の状況に適合しているか、最新の法律や企業や組織の現状を踏まえ、情報セキュリティポリシーに不備や不足はないか、なども考慮する必要があります。

見直しと改訂

評価、監査、調査の結果、社員や職員からの要求に基づいて、情報セキュリティポリシーの見直しと改訂を行います。改訂した情報セキュリティポリシーは、再び計画のプロセスを経て、運用に移していきます。

事故やトラブル発生時の対応

情報セキュリティに関わる事故やトラブルが発生した場合には、情報セキュリティポリシーに記載されている対応方法に則して、適切かつ迅速な処理を行うことこそが、被害や損失を最小限に抑える最大の対策です。

昨今ではBCP（事業継続計画）を策定することも多いですが、その観点で事故やトラブルの対応方法を策定しておくことも有効です。

事故やトラブルが発生した場合には、以下の手順で対応します。なお、ここでは、ネットワークへの不正侵入を例として取り上げることにします。

(1) 事故の検知

定期的なログチェックや障害検知ツールの利用によって、不審な状況の発生を検知する。
また、社内外からの通報窓口の整備も有効。外部でないと分からないインシデントもあるため、社外からの窓口が有効だが、通報用メールアドレスで適切な担当に届かないケースもあり、確認が必要。

(2) 事故の初動処理

関連する部署や担当者へ連絡を行い、あらかじめ設定した優先順位によって手続を行う。情報が漏洩（ろうえい）しているなどの危険があれば、この段階でホームページを閉鎖する、データをインターネットに接続されていないパソコンに退避するなどの処置が必要である。なお、利用者に被害が及ぶ可能性がある場合には、速やかに利用者に連絡を行う。

また、この段階でセキュリティ対策機関等への情報提供も強く望まれる（情報提供先はリンク集に記載）。早期の情報提供により、同様のサイバー攻撃の被害を防げた例もある。取引先などの関係先にも情報提供を行うことが望まれる。

(3) 事故の分析

被害内容や事故の規模を整理して、事故が発生した原因を分析し、対応策を決定する。

(4) 復旧作業

システムを復旧して、正常に動作していることを確認する。復旧が完了したら、関係者や利用者への連絡を行う。

(5) 再発防止策の実施

原因を究明して、同様の事故が再発しないように対策を講じる。事故に対する処理や対策で必要な項目については、情報セキュリティポリシーに反映する。

組織幹部として、これらの一連の処理の中でもっとも重要なことは、常に状況を判断できるような情報伝達の手順やルールを確立しておくことです。過去に発生した情報漏洩事件などでは、組織幹部への情報伝達が遅れたり、正確な情報が伝わらなかったりしたために、もっとも大切な初動処理にミス

が発生して、事故の被害をさらに拡大させてしまっているケースが数多く見受けられます。

これらの情報セキュリティに関する事故の事例を参考にして、適切な対応が可能な情報伝達や対応方法を手順やルールとして情報セキュリティポリシーに組み込んでおくことで、情報セキュリティ対策をさらに強化することができます。

しかし、実際にトラブルが発生した場合は、事前に策定した手順通りにはいかないことも多々あります。その際は、経営判断が求められることとなります。一例を挙げれば、復旧のために通常業務をいつまで、どの範囲まで止めるのかといった判断があります。さらに例を挙げれば、ランサムウェアの被害に遭った際、通常は支払うものではないとされる身代金について、人命がかかっている等の緊急時には敢えて支払う判断もあり得ます。

これらの判断は、情報セキュリティ担当部署や担当者に任せられるものではなく、経営側が判断を下す必要があることを意識しておく必要があります。

個人情報取扱事業者の責務

個人情報保護法は、個人の権利と利益を保護するために、2005年4月から全面施行された法律で、個人情報を保有する事業者が遵守すべき義務などを定めた法律です。

個人情報取扱事業者の責務

「個人情報取扱事業者」とは、個人情報保護法第2条第3項において、「個人情報データベースなどを事業の用に供している者」と定義されています。また、「個人情報」とは、生存する個人に関する情報のことで、氏名、生年月日などのデータによって特定の個人を識別できる情報又は個人識別符号（※）を含む情報のことを指しています。

（※）個人識別符号とは

- 身体の一部の特徴をコンピュータで利用するために変換したもの（たとえば、DNAや顔など）
- 公的なサービスの利用のためにサービス利用者に割り振られる番号（たとえば、免許証の番号やマイナンバーなど）

のことです。

個人情報保護法では、個人情報取扱事業者に対し、以下のことを義務付けています。

- 個人情報を取り扱うに当たっては利用目的をできる限り特定し、原則として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ってはならない。
- 個人情報を取得する場合には、利用目的を通知・公表しなければならない。なお、本人から直接書面で個人情報を取得する場合には、あらかじめ本人に利用目的を明示しなければならない。
- 個人データを安全に管理し、従業員や委託先も監督しなければならない。
- あらかじめ本人の同意を得ずに第三者に個人データを提供してはならない。
- 事業者の保有する個人データに関し、本人からの求めがあった場合には、その開示を行わなければならない。
- 事業者が保有する個人データの内容が事実でないという理由で本人から個人データの訂正や削除を求められた場合、訂正や削除に応じなければならない。
- 個人情報の取扱いに関する苦情を、適切かつ迅速に処理しなければならない。

匿名加工情報とは

匿名加工情報とは、個人情報を加工して、通常人の判断をもって、個人を特定することができず、かつ、加工する前の個人情報へと戻すことができない状態にした情報のことです。

匿名加工情報には、個人情報に関するルールは適用されず、一定の条件の下、本人の同意をとらなくても自由に利活用することができます。これにより、新事業や新サービスの創出や、国民生活の利便性の向上が期待されます。

事業者は、匿名加工情報を作成する場合、第三者に提供する場合、第三者から受領する場合における各ルールを守る必要があります。

(1) 匿名加工情報を作成する場合

- 適正な加工
- 削除した情報や加工の方法に関する情報の漏洩を防止するための安全管理措置
- 匿名加工情報に含まれる情報の項目の公表
- 加工前の個人情報における本人の特定禁止
- 苦情の処理等(努力義務)

(2) 匿名加工情報を第三者に提供する場合

- 匿名加工情報に含まれる情報の項目と提供の方法の公表
- 提供先に対する匿名加工情報であることの明示

(3) 匿名加工情報を第三者から受領した場合

- 加工前の個人情報における本人の特定禁止
- 加工方法の取得禁止
- 苦情の処理等(努力義務)

罰則等

なお、個人情報保護委員会は、個人情報取扱事業者や匿名加工情報取扱事業者に対し、個人情報の取扱いに関し報告させることができ、また、個人情報取扱事業者や匿名加工情報取扱事業者が上記の義務に違反している場合などには、当該事業者に対し、必要な措置をとるべきことを命じることができます。個人情報保護委員会の命令に違反した場合や、報告義務に違反した場合には、以下の罰則が科せられます。

- 個人情報保護委員会の命令に違反した場合6ヶ月以下の懲役又は30万円以下の罰金
- 報告義務に違反した場合30万円以下の罰金

個人情報の取扱いに関する詳細については、個人情報保護委員会のサイトにガイドラインや相談窓口など有用な情報が掲載されています。

https://www.ppc.go.jp/

このテキストに関する問い合わせ先

総務省 サイバーセキュリティ統括官室
Email:kokumin-security@ml.soumu.go.jp

- 国民のためのサイバーセキュリティサイト
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
- キッズページ
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/
- このテキストの利用規約
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/guide.html