

YKK グループ会社は、個人情報について、以下の安全管理措置に基づき管理する。

#### 第1（基本方針の策定）

個人情報の適正な取扱いの確保について組織として取り組むために、基本方針を策定する。

#### 第2（個人情報の取扱いに係る規律の整備）

取り扱う個人情報の漏えい等の防止その他の個人情報の安全管理のために、個人情報の具体的な取扱いに係る規律を整備する。

#### 第3（組織的安全管理措置）

##### (1) 組織体制の整備

安全管理措置を講ずるための組織体制を整備する。

##### (2) 個人情報の取扱いに係る規律に従った運用

あらかじめ整備された個人情報の取扱いに係る規律に従って個人情報を取り扱う。なお、必要に応じ、整備された個人情報の取扱いに係る規律に従った運用の状況を確認するため、システムログ又は利用実績を記録する。

##### (3) 個人情報の取扱状況を確認する手段の整備

個人情報の取扱状況を確認するための手段を整備する。

##### (4) 漏えい等事案に対応する体制の整備

漏えい等事案に対しては、漏えい等告示に準じて対応する。

##### (5) 取扱状況の把握及び安全管理措置の見直し

個人情報の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む。

#### 第4（人的安全管理措置）

従業員に、個人情報の適正な取扱いを周知徹底するとともに適切な教育を行う。

#### 第5（物理的安全管理措置）

##### (1) 個人情報を取り扱う区域の管理

個人情報にかかる個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（以下「管理区域」という。）及びその他の個人情報を取り扱う事務を実施する区域（以下「取扱区域」という。）について、それぞれ適切な管理を行う。

##### (2) 機器及び電子媒体等の盗難等の防止

個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行う

##### (3) 電子媒体等を持ち運ぶ場合の漏えい等の防止

個人情報が記録された電子媒体又は書類等を持ち運ぶ（個人情報の管理区域又は取扱区域からの持出し又は管理区域又は取扱区域への持込みをいう。）場合、容易に個人情報が判明しないよう、安全な方策を講じる。

##### (4) 個人情報の削除及び機器、電子媒体等の廃棄

個人情報を削除し又は個人情報が記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行う。個人情報を削除した場合、又は、個人情報が記録された機器、電子媒体等を廃棄した場合には、削除

又は廃棄した記録を保存する。それらの作業を委託する場合には、第7条に基づく監督をすることに加え、委託先が確実に削除又は廃棄したことについて証明書等により確認する。

## 第6（技術的安全管理措置）

### (1) アクセス制御

担当者及び取り扱う個人情報にかかる個人情報データベース等の範囲を限定するために、適切なアクセス制御を行う。

### (2) アクセス者の識別と認証

個人情報を取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。

### (3) 外部からの不正アクセス等の防止

個人情報を取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。

### (4) 情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人情報の漏えい等を防止するための措置を講じ、適切に運用する。

## 第7（委託先に対する監督責任）

個人情報の取扱いの全部又は一部を委託する場合は、委託を受けた者に対し、委託者として必要かつ適切な監督を行うため、次に掲げる措置をとるものとする。

1. 委託先の選定に当たっては、委託先の安全管理措置が、本「安全管理措置」と同等であることを確認するため、本「安全管理措置」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認する。
2. 選定した委託先とは委託契約を結ぶものとし、委託契約には、当該個人情報の取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人情報の取扱状況を委託元が合理的に把握することを可能にする規定を盛り込む。
3. 委託先における委託された個人情報の取扱状況を把握するため、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、委託先における委託された個人情報の取扱状況を適切に評価する。
4. 委託先による再委託は禁止する。

## 第8（漏えい等についての対応）

個人情報が万が一漏えい、滅失、改ざんされ、又はその恐れがある場合には、以下の措置を講じる。

### (1) 内部における報告及び被害の拡大防止

責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

### (2) 事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

### (3) 影響範囲の特定

上記(2)で把握した事実関係による影響の範囲を特定する。

### (4) 再発防止策の検討及び実施

上記（２）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を速やかに講ずる。

(5) 影響を受ける可能性のあるご本人への連絡等

漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係等について、速やかにご本人へ連絡し、又はご本人が容易に知り得る状態に置く。

(6) 事実関係及び再発防止策等の公表

漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する。

(7) 監督機関への通知

漏えい等事案の内容等に応じて、当該法域の適用のある法令において要求されている場合には、速やかに（遅くとも適用のある法令の定める期限までに）監督機関に報告する。

以上