別紙

下記１，２に基づき、貴社及び委託先等の事業者における個人情報の適正な取扱いに万全を期するとともに、以下の点について、特段の注意を払うこと。

○経営者が率先して、自社内における個人情報の管理体制を構築し、役員クラスの責任者への任命や、個人情報を取り扱う専門部署の設置等、十分な措置を講じること。
○委託先の安全管理措置の実施が十分かを確認すること。また、委託先が再委託をする場合には、事前に承認を求めるようにするとともに、再委託先による安全管理措置の実施が十分かを確認すること。再々委託先以降についても同様の扱いとすること。
○第三者から個人情報を取得する場合には、当該情報について、その入手方法等を確認すること。適法に入手されていることが確認できないときには、偽りその他不正の手段により取得されたものである可能性もあることから、取引の自粛を含め、慎重に対応すること。

記

１．個人情報保護法に基づく個人情報取扱事業者の守るべきルールの徹底

個人情報の適正な取扱いを行うべく、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」に沿った点検を行う。その際、例えば、以下のような項目について、十分チェックを行う。

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

○個人情報の利用目的の特定（法第 15 条）、目的外利用の禁止（法第 16 条）
個人情報を取り扱うに当たっては、利用目的をできるだけ特定しなければならない。また、特定された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。

○適正な取得（法第 17 条）
偽りその他不正な手段によって個人情報を取得してはならない。

○取得時の利用目的の通知等（法第 18 条）
個人情報を取得したときは、本人に速やかに利用目的を通知又は公表しなければならない。また、本人から直接書面で取得する場合には、あらかじめ本人に利用目的を明示しなければならない。

○個人データ内容の正確性の確保（法第 19 条）
利用目的の範囲内で、個人データを正確かつ最新の内容に保つよう努めなければならない。
◆具体的な措置例
・個人データ入力時の照合・確認手続の整備
・記録事項の更新
・保存期間の設定　等

○安全管理措置（法第 20 条）

個人データの漏えいや滅失を防ぐため、必要かつ適切な安全管理措置を講じなければならない。

◆具体的な措置例

・セキュリティ確保のためのシステム・機器等の整備

・事業者内部の責任体制の確保（個人情報保護管理者の設置、内部関係者のアクセス管理等）等

○従業者・委託先の監督（法第 21-22 条）

安全に個人データを管理するために、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。また、個人データの取扱いについて委託する場合には、委託先に対し必要かつ適切な監督を行わなければならない。

◆具体的な措置例

・個人情報保護意識の徹底のための教育研修等の実施

・個人情報保護措置の委託契約内容への明記

・再委託の際の監督責任の明確化　等

◆従業者とは、正社員のみならず、役員、契約社員、アルバイト等も含む。

◆委託元での安全管理措置（法第 20 条）と同等の措置が委託先でも講じられるような監督が求められる。

◆再委託の場合、委託先が適正な再委託先を選定しているか、委託先が再委託先に対して十分な監督を行っているかなど、委託元は把握し、適切な指導をする必要がある。

２．内部関係者の不正行為による情報漏えいを防止するセキュリティ対策の徹底

内部不正による情報漏えいを防止するための適切なセキュリティ対策を講じるべく、独立行政法人情報処理推進機構（IPA）が策定した「組織における内部不正防止ガイドライン」に沿った点検を行う。その際、チェックシートの活用とともに、例えば以下のような項目について、十分チェックを行う。

なお、個人情報を含む営業秘密の漏えいに関しては、「営業秘密管理指針」において、不正競争防止法上の営業秘密として保護を受けるために望ましい管理方法等が示されているので、営業秘密についてはこちらに沿った点検も行う。

組織における内部不正防止ガイドライン
http://www.ipa.go.jp/security/fy24/reports/insider/
セキュリティ対策の見直しに関する注意喚起文（7 月 10 日）
http://www.ipa.go.jp/security/announce/20140710-insider.html
営業秘密管理指針
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216hontai.pdf

〇アクセス権指定

重要な情報が保管されているファイルやデータベースについて、適切なアクセス権限を付与すること。

〇物理的管理

重要な情報が保管されているファイルやデータベースについて、情報の持ち出し・可搬媒体等の持ち込みの監視を行うこと。

〇証拠確保

重要な情報が保管されているファイルやデータベースについて、定期的な操作履歴の監視・監査を行うこと。