外部委託先管理規程

1.0版

外部委託先管理規程

外部委託先管理規程

１　趣旨

本規程は、当社の業務を外部の業者に委託し、実施する場合の契約における問題および委託先を管理する上での問題を未然に防ぐことを目的とする。

２　対象者

委託を行うすべての従業員。

３　対象システム

委託業務で使用するすべてのもの。

４　遵守事項

４．１　委託先の選定に関する遵守事項

（１）　委託を行う者は、委託先として信頼できる業者を選ばなければならない。

・委託先の選定基準を作成し、その基準に従い委託先を選定すること、又委託先に周知すること。

・選定基準を定期的に見直すこと。

・選定先が基準に適合しているか定期的に見直しを行い不具合があれば是正処置を施すこと。

４．２　委託契約に関する遵守事項

(A.13.2.4、A.14.2.7、A.15.1.1)

（１）委託を行う者は、委託業務の仕様以外に、機密保持及び守秘義務、その他関連する以下の契約事項を盛り込まなければならない。

① 秘密保持契約又は守秘義務契約の内容

・保護される情報の定義（例えば、秘密情報）

・秘密を無期限に保持する場合も含めた、契約の有効期間

・契約終了時に要求する処置

・認可されていない情報開示を避けるための、署名者の責任及び行為

・情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連

・秘密情報の許可された利用範囲、及び情報を利用する署名者の権利

・秘密情報に関する行為の監査及び監視体制

・許可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス

・契約終了時における情報の返却又は破棄に関する条件

・契約違反が発生した場合にとるべき処置

② 外部委託先による開発の内容

・外部委託した内容に関連する使用許諾に関する取り決め、コードの所有権及び知的財産権

・セキュリティに配慮した設計、コーディング及び試験の実施についての契約要求事項

・外部開発者への、承認済みの脅威モデルの提供

・成果物の質及び性格さに関する受け入れ試験

・セキュリティ及びプライバシーについて、容認可能な最低限のレベルを定めるためのセキュリティしきい（閾）値を用いていることを示す証拠の提出

・引渡しに当たって、悪意のある内容（意図的なもの及び意図しないもの）が含まれないよう十分な試験が実施されていることを示す証拠の提出

・既知の脆弱性がふくまれないよう、十分な試験が実施されていることを示す証拠の提出

・預託契約に関する取決め、例えば、ソースコードが利用できなくなった場合

・開発プロセス及び管理策を監査するための契約上の権利

・成果物の作成に用いたビルド環境の有効な文書化

・適用される法律の遵守及び管理の効率の検証については、組織が責任を負うこと

③ 供給者関係の内容

・組織が、自らの情報へのアクセスを許可する供給者の種類（例えば。ＩＴサービス、物流サービス、金融サービス、ＩＴ基盤の構成要素などの供給者）の特定及び文書化

・供給者関係を管理するための標準化されたプロセス及びライフサイクル

・様々な供給者に許可される情報へのアクセスの種類の定義、並びにそのアクセスの監視及び管理

・情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスクプロファイルに基づく供給者との個々の合意の基礎となるもの

・それぞれの供給者及びアクセスに関して確立した情報セキュリティ要求事項が順守されているか否かを監視するためのプロセスおよび手順、これには第三者のレビュー及び要求事項が順守されているか否かを監視うるためのプロセス及び手順、これには第三者おレビュー及び製品の妥当性確認も含まれる

・各当事者が提供うる情報又は情報処理の完全性お確実にするための、正確さ及び全さの管理

・組織の情報お保護するために供給者に適用する義務の種類
・供給者によるアクセスに伴うインシデント及び不測お事態への対処、これには、組織及び供給者の責任も含める
・各当事者が提供する情報又は情報処理お可用性を確実にするための、対応力に関する取決め、並びに必要な場合には、回復及び不測の事態に関する取決め
・調達に関する組織の要員を対象おした、適用あれる方針プロセス及び手順についての意識向上訓練
・供給者の要員とやり取りする組織お要員お対象とした、関与及び行動に関する適切な規則（これは、供給者の種類、並びに組織のシステム及び情報への供給者によるアクセスのレベルに基づく。）についての意識向上訓練
・情報セキュリティに関する要求事項及び管理策を、両当事者が署名する合意書の中に記載する条件
・情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実性

（２）委託を行う者は、委託業務の仕様以外に、品質管理に関する以下の契約事項を盛り込まなければならない。

① 委託業者は、スケジュールに従った作業を実施し、途中経過における進捗状況を明確にしなければならない。

委託業者は、品質管理のために実施する事項を明確にしなければならない。

（３）委託を行う者は、委託業務の仕様以外に、再委託に関する以下の契約事項を盛り込まなければならない。

① 委託業者が、再委託を行うためには、当社に事前の承認を得なければならない。

４．３　委託先の管理に関する遵守事項

（１）委託先の契約、基準、その他の契約事項等を定期的に見直しすること。
（２）契約事項が遵守されている事を定期的に監査すること。
（３）委託先が委託先の従業員に対し、必要な教育を行っているか定期的に監査すること。

４．４　委託先のクラウドサービスの利用に関する遵守事項

（１）クラウドサービスに要求するセキュリティレベル、サービスレベルを確認する。
（２）クラウドサービスのユーザインターフェイスの変更、機能変更・追加に注意し、認証などセキュリティ強化に繋がる変更は利用する。
（３）データセンターのロケーションにより適用される法律が違うことに注意する。

（4）公的な機関が提供するクラウド選定基準、ガイドライン等参照すること。

５　運用確認事項

５．１　委託先選定に関しての確認事項

（1）定期的に選定基準及び選定先の見直しが行われている事を確認する。

（2）定期的に監査が実施されているか確認すること。

（3）委託先管理に関する環境の変化が生じた時、関連業務が見直しされていることを確認すること。

５．２　委託先契約に関しての確認事項

（1）契約事項等か定期的に見直されているか確認すること。

５．３　委託先の管理に関しての確認事項

（1）基準及び契約事項等が定期的に見直されている事を確認する。

（2） 契約事項等が遵守されていることを定期的に確認する。

（3）従業員への教育が実施されているか確認する。

（4）情報セキュリティへの取組み及び委託先の情報セキュリティ対策状況を確認、すること。

（5）対外的な関連の為、書類は厳正に確認し適正に処理保管する事、又確認事項等での内容は書類で残し且つ相手先との確認のサインを残すこと。

５．４　委託先のクラウドサービスの利用に関しての確認事項

（1）定期的に監査を行い基準等が適切に運用されている事を確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。