2021 年 11 月 12 日
日本メックス株式会社

情報取扱い要領

委託先（パートナー会社）の皆様には、基本契約／契約約款に基づき、弊社から提供する情報の管理及び再委託会社の管理を行って頂いております。この度、情報の取り扱いの詳細を「情報取扱い要領」として取りまとめましたので、本要領に基づき、情報の確実な管理を行うことにします。

１．組織／体制

(1) 情報セキュリティの責任者、担当者を配置する。
※情報セキュリティの責任者が担当者を兼務しても良い。

(2) 情報システムの担当者を配置する。
※上記(1)の情報セキュリティの責任者又は担当者が兼務しても良い。

(3) 情報セキュリティに関する社内規程又は要領等を定め、運用する。なお、社内規程又は要領等は、定期的に見直しの検討を行い、必要に応じ改訂する。

2．業務従事者への教育・指導

(1) 業務従事者に対し、情報セキュリティ等に関する教育・指導を継続的に実施する。
（最低年 1 回もしくは契約期間が 1 年未満の場合は委託業務開始時）

(2) 業務従事者が退職等で業務を離れる際は、委託先内において、誓約書の取得、弊社業務に関する情報資産の返却確認を行う。

3．情報システムの対策

(1) 外部からの社内ネットワークへの不正アクセスを防止する。

(2) 電子ファイルは、アクセス権を設定しているファイルサーバ等に格納する。

(3) サーバや PC にウィルス対策ソフトを導入し、パターンファイルの更新を定期的に行う。

(4) 情報システム（Windows、ソフトウェア等）に対して、修正プログラムの適用、Windows update 等を行い、脆弱性の解消を行う。

(5) 私物のスマートフォン／携帯電話／タブレット等で、工事現場等の撮影、画像送信を行わない。

(6) PC、外部記憶媒体（SD カード、USB メモリ等）の利用は、会社貸与品のみとし、個人所有のものを使用しない。

(7) 社外等での UBS メモリ等の利用時には、情報を暗号化する。

4．重要情報の取扱い

(1) 弊社から重要情報として指定された秘密情報（機密情報）（以下、「重要情報」という。）の提供を受けた場合、重要情報管理表で管理する。
※重要情報：設計図書等、個人情報、日本メックスが指定した情報

(2) 重要情報を含め秘密情報（機密情報）は、目的外のことに利用しない。

(3) 重要情報を配布（複製・複写）する際には、委託元の承認後に配布する。なお、配布する際には、いつ、誰が、誰に、どのような方法で配布したか等を記録する。

(4) 重要情報の社外持出しは、原則、禁止とする。（特に、自宅への持出しは、絶対に行わない。）やむを得ず、重要情報を社外に持出す際は、委託先での承認ルールに基づき、承認を得る。

(5) 重要情報が記録された紙媒体、外部記憶媒体（UBS メモリ、SD カード、CD、DVD 等）は、常時、施錠可能な書庫等に保管する。

(6) 重要情報は、業務上不要になった時点で弊社へ返却、もしくは廃棄・削除する。

5．再委託先の管理

(1) 弊社が求める情報セキュリティ要件（本要領等）を再委託先が満たしていることを確認する。

(2) 再委託先に重要情報を提供する場合、弊社の承認を得る。

(3) 再委託先へ提供する重要情報は、目録（情報授受記録等）で管理する。

(4) 重要情報は、業務上不要になった時点で再委託先から返却、もしくは廃棄・削除していることを確認する。

6．情報セキュリティ事故

(1) 情報セキュリティ事故（情報紛失、情報漏洩等）の発生時は、弊社に速やかに報告する。

(2) 委託先内の情報共有、委託元への報告等の連絡網を整備する。

(3) 弊社に再発防止策を報告し、対策後、再発防止策の有効性評価を行う。

7．自主点検／監査

(1) 情報セキュリティの対策状況について、自主点検又は内部監査を行う。（最低年 1 回）
なお、弊社からの案件受託時には、「＜委託先＞情報セキュリティチェックシート」（別紙 2）に基づき、自主点検を行う。
■「＜委託先＞情報セキュリティチェックシート」（別紙 2）の掲載先
・日本メックスのホームページ：https://www.meccs.co.jp/partner/

(2) 上記(1)の情報セキュリティの対策状況の自主点検結果は、弊社からの依頼に応じ、提出する。

(3) 委託先にて内部監査を実施している場合、弊社からの依頼に応じ、内部監査の結果を提供可能な範囲で報告する。

(4) 自主点検又は内部監査の結果に基づき、継続的改善を行う。

以上