情報セキュリティ個別方針

1. 情報資産管理

当社のISMS適用範囲で使用する情報資産を適切に管理するため、使用する情報資産を洗い出し、情報資産の重要度(リスクが顕在化した場合の影響度)に応じたリスク対策を決定し、実施する。

リスク対策を適切に実施するため、対象となる情報資産の責任者を明確にし、影響度に応じた分類とそのラベル付け、及び取り扱いの基準を定め実施する。

情報資産利用の許可範囲を、「部屋、区画、建物、施設、拠点等」の物理的範囲、「業務機能、部門、職位、職階、プロジェクト」等の組織的範囲、「構内 LAN、広域 WAN、VLAN、区画分割」等ネットワークの技術的範囲の観点で定め管理する。特に、ISMS 適用範囲外への情報資産持ち出しや、テレワーク・インターネット利用等の外部ネットワーク接続に関しては許認可プロセスを確立する。

可用性が重要な情報資産は、適切なバックアップを取得し、安全な場所に保管する。

情報資産の処分(廃棄)にあたり、情報資産に対する不適切な取り扱いのリスクを防止するために、記録された情報(消去されたデータ含む)を完全に消去、又は物理的に破壊(消磁を含む)する手順を確立し実施する。情報資産の処分(廃棄)、及び再利用を第三者に委託する場合には、信頼できる委託先であることを確認した上で、情報セキュリティ条項を入れた契約を締結し、委託契約の履行について、委託の都度証明を受領する。

2. 組織的人的セキュリティ

当社のISMS運用に関わる従業者の役割・責任を明確にし、その遂行を業務として各従業員に割り当てる。

当社の ISMS 適用範囲で業務に従事する従業者は、業務に従事する前に、ISMS に関する基礎知識を持ち、当該業務に関わる情報セキュリティ対策と、従業者自身の役割と責任を認識しなければならない。そのために当社は、ISMS に関する新入社員教育(新卒及び中途採用)と定期教育を実施する。また、ICT 設備(サーバ、PC、タブレット、スマートフォン、通信設備等)の導入及び運用と、情報システム開発及び運用に関わる従業者に対し、技術的教育を力量管理の一環として実施する。

従業者の雇用(又は契約)の終了・変更の際に、継続して順守すべき情報セキュリティの責任を伝達するとともに、権利を喪失したアクセス権の削除・変更及び、当該従業者が所持する全ての会社資産の返却手続きを確立し、実施する。

3. アクセス制御

当社が保有・保管する情報資産に対するアクセスは、業務上の必要性及びリスク対策上の必要性を考慮し、物理的範囲・組織的範囲・技術的範囲の観点でアクセス権を設定する。

アクセス制御の運用では、許可された者(従業者、情報システムの処理プロセス、部門、お客様、取引先等)だけが情報資産にアクセス可能とするために、認証(本人確認)と認可(アクセス権限)の仕組みを整備する。

アクセス権の管理が適正であることを維持するために、定期的に ID の登録及びアクセス権付与の状況をレビューし、故意又は過失による不正な登録がないことを確認する。また、監査ログを取得し、重要な情報資産に対するアクセス権の行使が適正であることを定期的にレビューする。

4. 物理的環境的セキュリティ

情報資産を物理的に保護するために、物理的範囲を取り扱っている情報資産の重要度に応じて分類（レベル分け）し、「特別な許可のない者が入退出可能な区画」から、「特別に許可された者だけが入退出可能な区画」まで、規程等に「情報セキュリティ区画のレベルの定義」と、「区画のセキュリティレベル毎の入退出を管理するための境界の設定」と、「その物理的保護及び入退出規則と区画内での行動指針」を整備する。

重要な情報を取り扱う ICT 設備は、「物理的不正アクセス・地震や風水害等の災害」から保護するよう設置し保守する。また、電源やケーブル（電源、通信）、サーバ室の空調機等は「障害、切断、破壊、盗聴等」から保護できるように設置し保守する。

PC 等の記憶装置を内蔵した装置は、社内外を問わず「のぞき見、盗難、紛失等」のリスクから保護するための運用ルールを定め実施する。

5. 通信及び運用管理

重要な情報処理設備の運用においては、不正操作や誤操作を防止するために、職務及び設備の分割、操作手順書の整備、技術的脆弱性の管理等の対策を確立し、実施する。

システムの可用性及び完全性を維持するため、システム容量管理や情報資産のバックアップ等の対策を確立し、実施する。

マルウェア（悪意のあるコード及び認可されないモバイルコード等）からの保護のために、検出、予防及び回復のための対策（利用者の意識向上の重要性を含めて）を確立し、実施する。

あらゆる情報転送（宅配便、郵便、電子メール、オンラインストレージ等）において、リスクを認識し、適切な対策を確立し、実施する。

認可されていない情報処理活動の検知及び障害時の対策に使用するため、「イベントログ（システム使用状況、障害ログ等）」「実務管理者の作業ログ」を適切に取得し、定期的にレビューする。また、ログに対する不正アクセスから保護し、適切な期間保持する。

OS・アプリケーション・ICT 機器に関する脆弱性情報を適時に収集し、その対応の必要性について検討する。対応が必要な場合には、関連する業務やシステムへの影響を考慮しつつ、速やかに実施する。

6. システムの取得、開発及び保守

情報システムの取得、開発及び保守のプロセスにおいて、不正行為又は誤作業等に起因する情報セキュリティインシデントの発生を抑止又は検知するために、規程及び手順を策定し、実施する。

情報システムの実装にあたり、計画した情報セキュリティ要件を満たすことを確実にする。

インターネットを介して利用・提供するアプリケーションサービスは、そのリスクを認識し、適切な対策を確立し、実施する。

7. 供給者関係（外部委託及び第三者の提供するサービス）管理

業務を外部委託する場合、及び第三者が提供するサービスを利用する場合に、業務委託先又は、サービスの供給者がアクセス可能な情報資産と関連するリスクを特定し、情報セキュリティ要求事項を特定し、事前に供給者と合意し、実施する。また、供給者との合意内容を監視及びレビューし、合意内容の順守を確実にする。

8. 情報セキュリティインシデント管理

情報セキュリティ事象と弱点を早期に発見し、必要な場合に適切な対処を迅速に実施するため、情報セキュリティ事象の報告・評価手順を定める。また、インシデント発生の場合、再発を防止するための是正処置を検討し、実施する。また、インシデントに至らなかった情報セキュリティ事象及び弱点の解消のため、予防処置の必要性を検討(リスクアセスメント)し、実施する。

9. 情報セキュリティの継続

当社の ISMS 適用範囲の事業継続に重大な影響を与える事象(災害、パンデミック、テロ等)が発生した際に、事業継続が必要となる情報セキュリティ(情報システムの可用性、テレワーク環境の機密性、社会混乱時の物理的保護等)の継続計画を策定し、維持する。

10. 順守

情報セキュリティに関わる法令・規制又は契約上の義務を識別し、情報セキュリティ上の違反を防止するための活動を実施し、維持する。

当社が定める情報セキュリティ規則に対する順守を確実にするために、日常的な ISMS 活動の自主点検、定期的な技術的点検、及び内部監査を実施する。

2022 年 3 月 1 日

株式会社テラソフト

代表取締役社長

仁平　久