情報セキュリティ基本方針

株式会社ケントク（以下、当社）は、当社における全ての情報資産対する機密性、完全性及び可用性を確保する事を目的とし、情報資産の安全性・信頼性を担保することが責務であることを改めて自覚し、以下の方針に基づき全社で情報セキュリティに取り組みます。

1. 適用範囲

1-1 場所の範囲

当社の敷地内、当社の工事現場、専用通信回線で結ばれた範囲、当社の電気通信用電装設備、その他当社の情報を取り扱うことを主たる目的とする物的設備の範囲とする。

1-2 人的範囲

(1) 当社の取締役、従業員等、当社と雇用契約関係を持つ者（以下「当社従業員」という）を対象とする。

(2) 当社が外部事業者等の間で業務契約などを締結し、当社の保有情報を使用した業務を行わせる場合、別途定める「業務委託契約書」に本方針を尊守することを明記し契約を取り交わす。

(3) 雇用契約関係及び業務契約関係が終了した者においても、「秘密保持契約に関する誓約書」をその者との間で取り交わすなどして、本方針の対象とする。

2. 運営責任者

当社内における情報セキュリティを促進するため、経営者主導で組織的かつ継続的に次のことを行う。

(1) 情報資産が重大な脅威にさらされていることを示す変化の監視

(2) 情報セキュリティの事件・事故の見直し及び監視

(3) 情報セキュリティを強化するための主要な発議の承認

(4) 本方針の尊守の励行および違反に対する措置

3. 情報セキュリティ対策

情報資産に対する各種脅威（ウイルスや悪意あるソフトウエアなど）から情報資産を保護するために、次にあげる情報セキュリティ対策を実施するものとする。

3-1 保有情報の分類と管理

情報システムの利用者が適正に情報システムを運用するため、管理方法の対策を講じる。これにより権限を持たない者による不正な情報システムの運用やアクセスを防止する。

3-2 人的セキュリティ

当社従業員に本方針および関係法令の内容を周知徹底する等、十分な教育および啓発が行われるよう必要な対策を講じる。

また、業務委託するにあたり、委託業者による不正な情報資産の取り扱いを防止するための対策を講じる。

3-3 運用におけるセキュリティ対策

緊急時に迅速かつ適切な対応を可能とするための危機管理および情報セキュリティ対策の尊守状況を確認するための運用面の対策を講じる。

3-4 ウイルス及び悪意あるソフトウエアの予防及び検出

情報システムに対するウイルスや悪意あるソフトウエアなどの侵入を防止し、検出するため情報システムに予防の処置を講じることとし、さらに利用者には危険を知らせることを行う。

4. 違反及び事件・事故の報告義務

情報システムに携わるすべての者は、情報セキュリティの事件・事故及び法令違反、約違反があった場合には適切に対処し、再発防止に努める。

5. 従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取組みを確かなものにする。

2022年　8月　1日

株式会社ケントク

代表取締役　関　洋幸