情報セキュリティ基本ポリシー

Ver.　1．9

1．　この文書の目的

　この文書は、当社の情報セキュリティに対する基本ポリシー（情報セキュリティ基本ポリシー）を定めたものである。今後この文書を情報セキュリティのよりどころとして位置づける。

2．　基本声明

　この情報セキュリティ基本ポリシー（以下ポリシー）の趣旨は、内部的・外部的であるか、故意であるか偶発的であるかを問わないすべての脅威から、当社の情報資産を保護することにある。

3．　情報セキュリティの定義

　情報セキュリティとは、機密性、完全性、可用性を確保し維持することを言う。機密性、完全性、可用性とは次のような意味をもつ。

　機密性：アクセスを許可された者だけが、情報にアクセスできることを確実にすること。
　完全性：情報および処理方法が正確であること及び完全であることを保護すること。
　可用性：認可された利用者が、必要なときに情報及び関連する資産にアクセスできることを確実にすること。

4．　情報セキュリティの目的

　当社と顧客及び協力会社との取引において当社の安全性を維持するために、このポリシーの定期的運用を実施し、改善余地（脆弱性）のあるものに対し改善し安全性を実証することが目的である。全従業員に対し、セキュリティの重要性と意識の向上を図る。
　当社のポリシーは下記の要求事項を確実に遵守することである。

（1）　当社が保有する情報資産を認可されていない第三者アクセスから保護すること。
（2）　当社が保有する情報資産が認可されていない第三者に故意または不注意な行為を通して開示されないこと。
（3）　許可されていない第三者アクセスからの修正から保護した情報資産の完全性を保つこと。
（4）　当社が保有する情報資産の機密性を維持すること。
（5）　許可された利用者が必要な時に情報を利用（可用性の確保）できるようにすること。
（6）　法規制上の要求事項を遵守すること。
（7）　事業継続計画を策定し、維持し、実行可能な限りレビューすること。
（8）　情報セキュリティ教育・訓練を全従業員に対して定期的に実施すること。
（9）　情報セキュリティの違反とその疑いのある弱点がすべて報告され調査されること。

5．　適用範囲

当社の契約内容に基づき雇用され、適用範囲の対象となる情報資産との関わり合いを持つ全従業員は、この「情報セキュリティ基本ポリシー」を実施することに責任があるものとする。なお、この「情報セキュリティ基本ポリシー」を承諾した経営層の支持を得ているものとする。

（1）　適用範囲は以下の通りとする。
　① 本社内に格納されている情報資産すべて
　② 本社外に持ち出す情報資産すべて
　③ 本社外から持ち込む情報資産すべて
　④ 顧客先におけるセキュリティルールの遵守
　※　本社所在地は以下の通りとする。
　　東京都品川区東五反田5－26－5　ニッセイ五反田駅前ビル　4F

※　スコープは、ソフトウェア開発業務の管理

6.　セキュリティ基本方針

（1）　情報資産の脆弱性及び情報資産をリスクにさらす恐れのある脅威を管理するために、適切なリスクアセスメントを通して情報資産の価値を特定すること。

（2）　ISMSを計画・実施し、改善すべき点を改善することにより、リスクを許容可能な水準に維持すること。

（3）全従業員は、情報セキュリティに関連する契約条件を遵守すること。

（4）当社社員は、就業規則を遵守すること。

（5）全従業員は、ISMSで規定した規則を遵守すること。

（6）全従業員は、法規制を遵守すること。

7.　全従業員の責任と義務

ポリシーの運用は運用手段に従い、定期的に内部監査を行いポリシーが遵守されているか確認する。情報セキュリティ管理者（情報セキュリティ委員会）は、適切な基準及び実施手順に基づき、ポリシーの実施を促進する。全従業員は、本「情報セキュリティ基本ポリシー」を維持するために策定された手順に従わなければならない。全従業員は、事故及び特定された弱点を報告する責任を要する。

8.　経営者の責任と義務

経営陣はポリシーの遂行の為、積極的に情報セキュリティへ関与する。情報セキュリティを実施する為に必要な経営資源を決定し、これを提供する。責任の明確な割当て及び承認を通して、組織内における情報セキュリティの活動を積極的に支持する。

9.　罰則

情報資産の保護を危うくする故意の行為を行った場合は、懲戒処分／法的処分の対象となる。また、偶発的な情報資産の保護を危うくする行為を行った場合は、その程度により、罰則を科すものとする。

10. 関連文書

本文書では各規程の具体的な諸基準を参照する。

11. 情報セキュリティ委員会の設置

社内の情報セキュリティの向上を図るため、情報セキュリティ委員会を設置する。
その役割は、定期的に会議を開催し社内の情報交換に努めると共に、情報セキュリティ基本ポリシーの見直しと承認、組織全体にかかわる情報セキュリティの責任の見直しと承認、情報資産が脅威にさらされていないかどうかの監視、情報セキュリティを強化するための提案、事故が起きた際の対応策の検討及び解決、セキュリティに関する情報収集活動などを行うものとする。

12. 定期的見直し

経営陣は、このポリシーを作成しレビューを行う。ポリシーは、1年に1回または必要性が生じた場合に、レビューを行う。また、ポリシーの変更が生じた場合、下位（各種規程／各種手順書）の見直し、変更が必要な物はレビューを行う。ポリシー／規程／手順書のレビューが行われた物に対し、妥当性を確認する。