# 情報セキュリティ方針
（ISO27001）

## 1 経営者の意向声明

当社の資産をあらゆる脅威から守り、機密性、完全性、可用性を確保し、維持し、
事業継続を確実にするために『情報セキュリティ方針』を定める。
全従業員は、情報セキュリティの規程を熟知し、順守しなければならない。

## 2 情報セキュリティの定義

情報セキュリティとは、情報の機密性、完全性、可用性を維持し、資産を適切に保護すること。

### 情報セキュリティの3要素（C・I・A）

**機密性** 情報を保護すること
つまり、アクセスが認可された者だけが、情報にアクセスできることを確実にする。
Confidentiality

**完全性** 情報が正確で完全なこと
つまり、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。
Integrity

**可用性** 必要な時にいつでも使えること
つまり、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。
Availability

## 3 情報セキュリティの目的

◆情報セキュリティの目的は「人的」、「ソフト」、「ハード」、「事業継続」、「ISMSの推進体制の確立」の5つの観点について設定する。
◆全従業員の情報セキュリティに対する啓発及び重要性を認識するために情報セキュリティ教育を実施すること。
◆ウイルス及び他の悪意あるソフトウエアの予防及び検出。
◆法律上及び契約上の要求事項への適合。
◆システムのトラブルにおけるリカバリーの性能向上を図ること。
◆事業継続計画を充実させること。
◆資産の機密レベルに従った適切な取扱いをすること。

## 4 適用範囲

当社は、経営陣のもとに、本社及び東京支社があり、施設開発計画立案から、デザイン・設計・施工・運営支援、そして各種プロモーションまでの業務から派生する資産を保有している。ここでいう資産とは、紙媒体・外部記憶媒体・コンピュータ等装置内に記録されたデータ、技術者の保有するノウハウである。

## 5 リスク評価基準とリスクアセスメントの構造の確立

適用範囲における全ての資産を洗出し、その資産価値の評価を、脅威と脆弱性の分析及び情報セキュリティの定義に従いリスクアセスメントを実施する。

## 6 事業継続管理

当社の事業活動が、天災（震災）もしくはPC及びサーバマシンの故障及びウイルス感染によって、業務が中断することを想定したリスク管理策を計画する。

## 7 ISMS確立、維持するための経営

社長は、事業上の要求事項を満たし、かつ、情報セキュリティの目標を達成するための経営資源（人的資源、基盤、作業環境）を明確にし、利用できることを確実にする。

## 8 法律及び契約の要求事項の適合

全ての資産とその取扱いは、関係法令及び契約条項を順守する。

## 9 役員及び従業員の責任と義務

役員及び従業員は、この情報セキュリティ方針及び情報セキュリティマネジメントシステムに関する社内規定、手順書に従い規定（ルール）を順守し、かつ資産に対して事件・事故及び特定された弱点について報告する義務がある。

### 情報セキュリティの報・連・相

**報 告** 資産に対して事件・事故が発生した場合、トラブル報告書に記載し、セキュリティ委員会に報告する。

**連 絡** 問題発生による連絡（緊急連絡も含む）は、当社の連絡網で確実に連絡する。

**相 談** 資産に対して問題または気になることがあれば、セキュリティ連絡票に記載し、セキュリティ委員会へ相談する。なお、気づいた問題に対して、自ら試みることは決してしないこと。

## 10 情報セキュリティの教育

役員及び従業員は、情報セキュリティの教育及び訓練に参加することを義務とする。

## 11 罰則

当社の資産の保護を危うくする故意の行為を行った場合は、就業規則懲戒規定に基づき対処する。

## 12 見直し及び評価

情報セキュリティ方針の見直し及び評価は、定期的に必要に応じて行われるマネジメントレビューで実施し、常により良いものに改善を図る。

制定：2007年11月1日　改訂：2015年4月1日

株式会社 シード 代表取締役　西島昭男