

# 情報セキュリティポリシー



近年の電子媒体やネットワークを介して取り扱う情報の著しい拡大に伴い、災害、故障・障害、過失・故意（ハッキングを含む）等のインシデントによる情報の漏洩、紛失、破壊等が発生するリスクが高まっております。これらによるお客様（発注者）及び弊社における甚大な損失の発生を未然に防ぐべく、預託された情報資産、及び弊社の事業遂行に必要な個人情報等の安全・信頼性のある情報管理体制の構築を目的に、情報セキュリティポリシーを定めます。

## ✓ 当ポリシーに関する位置付け・適用範囲

当該ポリシーを情報セキュリティ対策の最上位に位置付け、当社業務の事業遂行に利用する情報資産、及び当社WAN・VPN、クラウドサービス、SNS、ビジネスチャット等の環境を利用する全ての社員及び関連会社等に適用します。

## ✓ 当社の情報セキュリティ体制

公共事業の一翼を担う企業の社会的責任として、『当然あるべき状態』を維持します。経営トップが情報セキュリティの最高責任者として方針を策定し、情報セキュリティ委員会が情報資産の運用・管理の全社的な情報セキュリティ体制を構築します。情報セキュリティ対策に関する指針の見直し、情報セキュリティ対策に関する予測インシデント（スパイウェアを含むウイルスの侵入・ハッキングなど、ネットワークからの侵入、社内・部外者による情報流出等）に対し予め対策を講じます。またホームページなどのビジネスサイト、情報共有の為のビジネスチャット等に関しては、SSL等の暗号化処理されたセキュリティ体制で維持・運営します。なお情報セキュリティ管理の一部を外部委託する場合は、当該ポリシーに従い管理させます。

## ✓ 情報の適切な取り扱いと管理

当社は、業務で預託された情報の重要性を認識のうえ関連法令等を遵守し、社内規定等のルールに則り情報資産の適正な利用と適切な管理を行います。

## ✓ 情報セキュリティ教育

情報セキュリティ教育の主たる目的は、当該ポリシーや関連法令・規定の周知徹底と考えます。情報セキュリティ対策を適切に運用し、情報セキュリティリテラシーを向上させるため、情報資産を利用する社員等に対し、脅威の情報や予防処置等に関する教育や啓発活動を継続的に行います。また協力会社に対しても情報セキュリティ教育を推奨します。

## ✓ 事故予防と対応

情報資産を利用する職員等は、各種リスクの重大性および情報セキュリティの重要性について十分認識し、情報資産の利用・管理に関わる事故等の予防に努めます。また万一事故が発生した場合には、再発防止策を含む適切な対策を速やかに講じます。

## ✓ 継続的改善

当社はこのポリシーに基づく対策を実践するとともに、継続的な見直しや内部監査活動を通じて、皆様から信頼される企業を目指します。また、継続的に情報セキュリティに対する新たなリスク等を評価し、適宜、情報資産保護・管理体制及び情報セキュリティポリシーを見直し、そのPDCAの実践に努めます。