独立行政法人中小企業基盤整備機構情報セキュリティ基本方針

機構の情報セキュリティ基本方針の策定について

機構の業務の遂行を行う上で必要となる情報セキュリティ対策についての原則的な事項を明示するものとして、情報セキュリティ基本方針を以下のとおり定める。

１．基本方針の策定の意義

独立行政法人中小企業基盤整備機構（以下、「機構」という。）は、個人情報、事業者の営業上又は技術上の権利に関わるもの等を取り扱っており、それらについて外部への漏えい、改ざん、消失等が発生した場合には、重大な社会的影響を招くおそれがある。

したがって、適切な情報セキュリティ対策を講じることにより、機構が取り扱う情報及び情報システム（以下、「情報資産」という。）を脅威から守ることは、機構の社会的信頼及び安定した事業運営の確保とともに機構の社会的使命を果たすうえで、必要不可欠である。

これゆえ、機構において遵守すべき情報セキュリティ対策の基本原則を示すものとして情報セキュリティ基本方針を策定し、必要かつ十分なセキュリティ対策を行うこととする。

２．情報セキュリティ対策の実施体制の確立

機構は、機構の情報資産に対する機構内外からの脅威を考慮し、それらに適切に対応が行える情報セキュリティ対策を行うため、必要な組織及び体制を整備し、責任と権限を明確にする。

３．情報セキュリティ対策の範囲

（１）基本方針において対象とする「情報資産」は、次に掲げるものとする。

①情報資産を構成する情報とは、次に掲げるものをいう。

イ　役職員等が職務上使用することを目的として機構が調達し、又は開発した情報システム若しくは外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

ロ　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、役職員等が職務上取り扱う情報

ハ　イ及びロのほか、機構が調達し、又は開発した情報システムの設計又は運用管理に関する情報

②情報資産を構成する情報システムとは、情報処理に係るシステム及び通信に係るシステムをいう。

（２）基本方針は、前項に掲げる情報及び情報システムを取り扱うすべての機構の役職員等に適用する。

（３）情報セキュリティ対策とは、情報の機密性、完全性及び可用性を維持することをいう。

４．基本方針の位置付け等

情報セキュリティ基本方針は、機構の情報資産に関する情報セキュリティ対策の原則的な事項について包括的に取りまとめたものであり、情報セキュリティ対策に関係する文書の最上位に位置する。

情報セキュリティ基本方針は、機構のすべての役職員等に情報を正しく取り扱わせるための意思統一を図ることを目的とするほか、機構の顧客が求める情報を正しく提供し、より良いサービスの実現に向けて努力するための根幹を担うものである。

また、情報セキュリティ対策を常に適切なものに維持していくためには、状況の変化等を的確にとらえ、それらに応じた情報セキュリティ対策の見直しを図ることが重要であることから、必要に応じてこの基本方

針及び関連する規程の見直しを行い、その妥当性を将来にわたり維持していくこととする。

５．基本方針に関係する規程の体系

（１）機構のセキュリティポリシーは、基本方針（本文書を指す）、基本方針の対策基準たる情報セキュリティ管理規程（以下、「管理規程」という。）の２層で構成するものとする。

（２）管理規程は、情報セキュリティ対策の基本的かつ具体的な対策基準を規定する。

（３）管理規程の実施に必要な具体的な実施手順として必要となる要領等は、それぞれ別途定めることとする。

６．情報セキュリティ対策の内容

（１）情報資産に関する対策

① 情報の分類と対策

情報をセキュリティの観点から内容により分類し、重要度に応じて対策を講じる。

② 情報のライフサイクルにわたる対策

情報の作成、入手、利用、保存、移送、提供、消去、廃棄等の情報のライフサイクルの各段階において必要な対策を講じる。

③ 情報セキュリティ要件に基づく対策

主体認証、アクセス制御、権限管理等の基本的なセキュリティ機能及び主要な脅威を防ぐために遵守すべき事項に関する必要な対策を講じる。

④ 情報システム及び保管施設・設備の構成要素についての対策

情報システムに係る装置、設備、ソフトウエア、施設・環境面等について必要な対策を講じる。

また、情報システムの開発に係る手続き、機構外での情報処理の制限等について必要な対策を講じる。

（２）役職員等に関する対策

① 情報セキュリティ対策に関する教育の実施

役職員等の新任時・異動時のほか、定期的に情報セキュリティ対策に必要な教育を行うものとする。

②　役職員等の責務

役職員等は、関係する法令を遵守するほか、情報セキュリティに関係する規程に定める事項の実施に責任を負うとともに、それらを遵守する。

③　関係者への周知及び徹底

役職員等は、外部委託先等、業務運営に関係する者に対してこの基本方針及び情報セキュリティに関係する規程の周知及び徹底を図るものとする。

７．用語の定義

この基本方針における用語の意義は、以下のとおりとする。

（１）「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。

（２）「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる状態を確保することをいう。

（３）「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。

８．　基本方針の公表

この基本方針は、機構の情報セキュリティ対策に対する考え方を外部に向けて明らかにするため、これを公表するものとする。