独立行政法人中小企業基盤整備機構情報セキュリティ管理規程

令和４年４月１日施行

第１条　（略）

（定義）

第２条　この規程において次の各号に掲げる用語の定義は、当該各号に定めるところによる。

一　「情報」とは、以下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、又は開発した情報処理若しくは通信の用に供する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。）

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

二　「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。

三　「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

四　「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。

五・六　（略）

七　「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機構が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。

八～二十三　（略）

第３条～第１２条　（略）

（対策推進計画）

第１３条　最高情報セキュリティ責任者は、第１９条第１項の評価の結果を踏まえた情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めなければならない。

２　機構は、対策推進計画に基づき情報セキュリティ対策を実施するものとする。

３　最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行わなければならない。

第１４条　（略）

（教育）

第１５条　機構は、役職員等が自覚をもってこの規程及び管理基準に定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行うものとする。

（情報セキュリティインシデントへの対応）

第１６条　機構は、情報セキュリティインシデントに対処するための体制として、CSIRT を構築するとともに、必要な措置を定め、実施するものとする。

２　情報セキュリティインシデントの可能性を認知した者は、上記体制の窓口に報告しなければならない。

３　この規程及び管理基準に定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じなければならない。

（自己点検）

第１７条　機構は、情報セキュリティ対策の自己点検を行うものとする。

（監査）

第１８条　機構は、管理基準がこの規程に準拠し、かつ実際の運用が管理基準に準拠していることを確認するため、情報セキュリティ監査を行うものとする。

（リスク評価と対策）

第１９条　機構は、第１７条の自己点検の結果、前条の監査の結果及びサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じるものとする。

２　機構は、前項の評価に変化が生じた場合には、情報セキュリティ対策を見直すものとする。

（情報の格付）

第２０条　機構は、取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付すものとする。

２　機構は、情報の提供、運搬及び送信に際しては、前項の情報の格付のうち、いかなる区分に相当するかを明示等するものとする。

（情報の取扱制限）

第２１条　機構は、情報の格付に応じた取扱制限を定めるものとする。

２　機構は、取り扱う情報に、前項で定めた取扱制限を付すものとする。

３　機構は、情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等するものとする。

（情報のライフサイクル管理）

第２２条　機構は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な措置を定め、実施するものとする。

（情報を取り扱う区域）

第２３条　機構は、機構が管理する又は機構以外の組織から借用している施設等について、機構の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施するものとする。

（外部委託）

第２４条　機構は、情報処理に係る業務を外部委託する際に管理基準で別に定める要機密情報を取り扱う場合には、必要な措置を定め、実施するものとする。

２　機構は、外部委託（約款による外部サービスの利用を除く。）を実施する場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めるものとする。

３　機構は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備するものとする。

（情報システムに係る文書及び台帳整備）

第２５条　機構は、情報システムに係る文書及び台帳を整備するものとする。

（情報システムのライフサイクル全般にわたる情報セキュリティの確保）

第２６条　機構は、所管する情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において、情報セキュリティを確保するための措置を定め、実施するものとする。

（情報システムの運用継続計画）

第２７条　機構は、情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案するものとする。

２　機構は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認するものとする。

（暗号・電子署名）

第２８条　機構は、機構における暗号及び電子署名の利用について、必要な措置を定め、実施するものとする。

（インターネット等を用いた事業サービスの提供）

第２９条　機構は、インターネット等を用いて事業サービスを提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を定め、実施するものとする。

（情報システムの利用）

第３０条　機構は、情報システムの利用に際して、情報セキュリティを確保するために役職員等が行わなければならない必要な措置を定め、実施するものとする。

第３１条・第３２条　（略）

以上