情報セキュリティ管理規程

平成 31 年規程第 25 号
平成 31 年３月 29 日制定
令和４年３月 10 日改正
令和６年４月 19 日改正
令和７年 12 月８日改正

第１章　目的及び適用対象

（目的）

第１条　この規程は、サイバーセキュリティ基本法（平成26年法律第104号。以下「法」という。）第26条第１項第２号に基づきサイバーセキュリティ戦略本部が作成する政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）を踏まえ、年金積立金管理運用独立行政法人（以下「管理運用法人」という。）が自らの責任において実施すべき対策を定めることにより、管理運用法人におけるサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。

（適用対象）

第２条　この規程の適用対象とする者は、管理運用法人の役員及び職員（臨時職員及び派遣契約職員を含む。以下「役員等」という。）とする。

２　この規程の適用対象とする情報は、役員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）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情報システムに入力された書面に記載された情報を含む。）及び情報システムの設計又は運用管理に関する情報とする。

第２章　情報セキュリティ対策のための基本方針

（管理体制）

第３条　管理運用法人は、情報セキュリティ対策を実施するための組織・体制を整備するものとする。

２　組織規程第２条の２第７号に定める最高情報セキュリティ責任者は、別に定めるところにより、同規程第２条の９第１項に定める自らの事務の一部を他の職員に行わせることができる。

（資産管理）

第４条　管理運用法人は、管理運用法人の情報資産の状況を把握し、情報セキュリティ対策に活用するため、保有する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。

（リスク評価と対策）

第５条　管理運用法人は、第10条に定める自己点検の結果、第11条に定める情報セキュリティ監査の結果、法に基づき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。

（対策推進計画）

第６条　最高情報セキュリティ責任者は、前条の評価の結果を踏まえた情報セキュリティ対策を組織的・継続的に実施し、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　管理運用法人は、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。

（例外措置）

第７条　管理運用法人は、情報セキュリティ対策の実施に当たり、例外措置を適用しようとするときは、必要な審査を行うものとする。

（教育）

第８条　管理運用法人は、役員等が自覚をもって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９条　管理運用法人は、情報セキュリティインシデントに対処するため、適正な体制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役員等は、別に定める報告窓口に報告しなければならない。

３　最高情報セキュリティ責任者及び下位規程で定める責任者は、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10条　管理運用法人は、情報セキュリティ対策の自己点検を行うものとする。

（情報セキュリティ監査）

第11条　管理運用法人は、関係規程等が統一基準群に準拠し、かつ実際の運用が関係規程等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。

（対策の見直し）

第12条　管理運用法人は、第５条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。

２　管理運用法人は、第５条の評価の結果又は前項の見直しを踏まえ、関係規程等の評価及び見直しを行うものとする。

３　最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査並びに法に基づきサイバーセキュリティ戦略本部が実施する監査等を総合

的に評価するとともに、情報セキュリティを取り巻く状況の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13条　管理運用法人は、厚生労働省より、関係規程等について同省における情報セキュリティ対策の基準を参考とするよう求められた場合は、必要に応じて関係規程等に反映させるものとする。

第３章　情報セキュリティ対策のための基本対策

（情報の格付）

第14条　管理運用法人は、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　管理運用法人は、外部の機関（以下「外部機関」という。）との情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、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15条　管理運用法人は、情報の格付に応じた取扱制限を定めるものとする。

２　管理運用法人は、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　管理運用法人は、外部機関への情報の提供、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16条　管理運用法人は、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17条　管理運用法人は、管理運用法人の事務所において情報を取り扱う区域の範囲を定め、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18条　管理運用法人は、管理運用法人の情報を取り扱わせる業務を委託する場合には、必要な措置を定め、実施するものとする。

２　管理運用法人は、業務委託を実施する際に要機密情報を取り扱わせる場合は、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　管理運用法人は、クラウドサービスを利用する場合には、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。

４　管理運用法人は、機器等の調達に当たり、機器等の開発等で不正な変更が加えられない

管理がなされている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定めるものとする。

（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19条　管理運用法人は、保有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20条　管理運用法人は、保有する情報システムに係る運用継続のための計画を整備する際には、業務継続計画及び関係規程等と整合性の確保を図るものとする。

（情報システムの利用）

第21条　管理運用法人は、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員等が行う必要のある措置を定め、実施させるものとする。

（関係細則等への委任）

第22条　この規程に定めるもののほか、この規程の実施のために必要な要件は、関係細則等で定める。

２　前項の関係細則等の制定及び改廃に当たっては、管理運用法人の業務の特性を踏まえつつ、統一基準群に準拠し、これと同等以上の情報セキュリティ対策が可能となるようにするものとする。

（規程の制定又は改廃）

第23条　この規程の制定、変更又は廃止は、経営委員会の議決により行うものとする。

附　則

この規程は、平成31年４月１日から施行する。

附　則（令和４．３.10 改正）

この改正は、令和４年４月１日から施行する。

附　則（令和６．４.19 改正）

この改正は、令和６年５月１日から施行する。

附　則（令和７.12.８改正）

この改正は、令和８年４月１日から施行する。