運用受託機関等における情報セキュリティ対策実施細則

平成31年細則第45号
平成31年３月29日制定

（目的）

第１条　この細則は、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。）の要機密情報を取り扱う者及び管理運用法人の管理運用業務に関する非公表情報を知り得る者の情報セキュリティ対策に関し必要な事項を定め、これらの者からの情報漏えいの防止を図ることを目的とする。

（定義）

第２条　この細則において、運用受託機関等とは、次の各号に掲げる者をいう。

（１）　運用受託機関

（２）　資産管理機関

（３）　委託調査研究の受託者及び共同研究の相手方

（４）　自家運用に係る債券の売買の取引先及び短期資産の運用先

（５）　情報システム関連業務の受託者

（６）　前各号に掲げる者のほか、管理運用法人の要機密情報を取り扱う者及び管理運用法人の投資行動に関する非公表情報を知り得る者（当該者の業務に関し法令により罰則を伴う秘密保持義務が課されている者を除く。）

（運用受託機関等の選定先等候補者への周知）

第３条　管理運用法人は、運用受託機関等に求める情報セキュリティ対策の内容をあらかじめ運用受託機関等の選定先等候補者（以下「候補者」という。）に周知する。

２　管理運用法人は、運用受託機関等において情報セキュリティが侵害された場合の対処方法をあらかじめ運用受託機関等の候補者に周知する。

３　管理運用法人は、運用受託機関等における情報セキュリティ対策の履行状況の確認のため情報セキュリティ監査を行う必要がある場合には、その内容及び方法等をあらかじめ運用受託機関等の候補者に周知する。

（運用受託機関等の選定）

第４条　管理運用法人は、運用受託機関等の選定に当たっては、管理運用法人と同水準以上の情報セキュリティ対策を実施できると認められる者を選定する。

２　管理運用法人は、運用受託機関等の候補者に対し、情報セキュリティ対策ベンチマークに

よる自己診断を求め、その結果を評価の要素とすることができる。ただし、運用受託機関等の候補者が情報セキュリティマネジメントシステム適合性評価制度に基づく認証又はこれと同等の認証を取得している場合は、これに代えることができる。

（再委託）

第５条　管理運用法人は、運用受託機関等がその業務の全部又は一部を他の事業者に再委託する場合は、運用受託機関等に対し、管理運用法人が運用受託機関等に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせるよう求める。

（秘密保持契約）

第６条　管理運用法人は、運用受託機関等に対して秘密保持に関する契約（以下「秘密保持契約」という。）を締結する。

２　秘密保持契約には、次の各号に掲げる事項を含めるものとする。

（１）　情報セキュリティを確保するための体制の整備に関する事項

（２）　運用受託機関等及びその従事者が業務の遂行上知り得た事実の漏えいの禁止に関する事項

（３）　業務の遂行上知り得た情報の複製等の制限に関する事項

（４）　業務の遂行上知り得た情報の目的外の利用禁止に関する事項

（５）　漏えい等の事案の発生時における対応に関する事項

（６）　再委託先における情報セキュリティ確保のための措置に関する事項

（７）　運用受託機関等に係る次のイからニまでに掲げる事項を記載した報告書に関する事項

イ　情報セキュリティ対策等を実施する管理体制

ロ　秘密保持契約で求める情報セキュリティ対策の実施に係る具体的な取組内容

ハ　管理運用法人に関する業務を担当する体制及び者（管理運用法人が必要と認める場合に限る。）

ニ　情報セキュリティに関する管理の体制及び状況についての検査又は監査に関する事項

（８）　前号の報告書の内容に変更があった場合の報告に関する事項

（９）　次条第２項及び第８条に規定する報告に関する事項

（１０）　前各号に掲げるもののほか管理運用法人に関する情報の保護に関し必要な事項

（情報セキュリティ対策の履行状況の確認）

第７条　管理運用法人は、運用受託機関等において情報セキュリティ対策が適正に履行されていることを確認するための方法を策定する。

２　管理運用法人は、運用受託機関等に対して定期又は随時に管理運用法人に関する情報に係る情報セキュリティ対策の履行状況を報告させる。

３　管理運用法人は、運用受託機関等の情報セキュリティに関する管理の体制又は状況に重大

な問題があると認めるときは、当該運用受託機関等との契約の解除等必要な措置を講ずるものとする。

（運用受託機関等による情報セキュリティ対策の自己診断）

第８条　管理運用法人は、少なくとも年に一度、運用受託機関等に対して、情報セキュリティ対策ベンチマークによる自己診断等を求め、その結果を報告させる。ただし、運用受託機関等が情報セキュリティマネジメントシステム適合性評価制度に基づく認証又はこれと同等の認証を取得している場合は、これに代えることができる。

（管理運用法人における評価及び報告）

第９条　管理運用法人は、第７条及び前条の結果その他の事実に基づき、運用受託機関等の情報セキュリティ対策を毎年度評価し、情報セキュリティ委員会及び内部統制委員会に報告する。

（成果の発表）

第10条　管理運用法人は、運用受託機関等が管理運用法人に関する内容及び成果を発表しようとする時は、書面によりあらかじめ管理運用法人の同意を得させる。

（適用除外）

第11条　最高情報セキュリティ責任者は、特別の事情があると認める場合は、この細則の一部を適用しないことができる。

２　管理運用法人は、この細則に定めるもののほか、委託業務の実施に関し必要があると認める事項は、運用受託機関等との合意により別に定めることができるものとする。

（細則の制定又は改廃等）

第12条　この細則の制定、変更又は廃止は理事長が定める。また、必要に応じて、理事長は本細則の下位規程を定める。

附 則

この細則は、平成31年４月１日から施行する。