（参考１）現状の業務リスク重要度

大 （中期目標の達成が困難）	2 8 13b 13d 29 30 中	3a 13a 13c 18 28 6 22 大	1 12 26 大
中 （中期目標に影響があるが期間内でのリカバリーが可能）	10 23 31 小	3b 7 9 16 20 21 25 中	4 5 11 15 17 19 24 27 大
小 （中期目標への影響はほとんどない）	小	小	14 中
影響度 ／ 発生頻度	少 （ほとんどない）	中 （年に1、2回程度）	多 （四半期に1、2回程度）

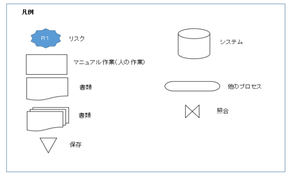
（参考２）現状の業務リスク

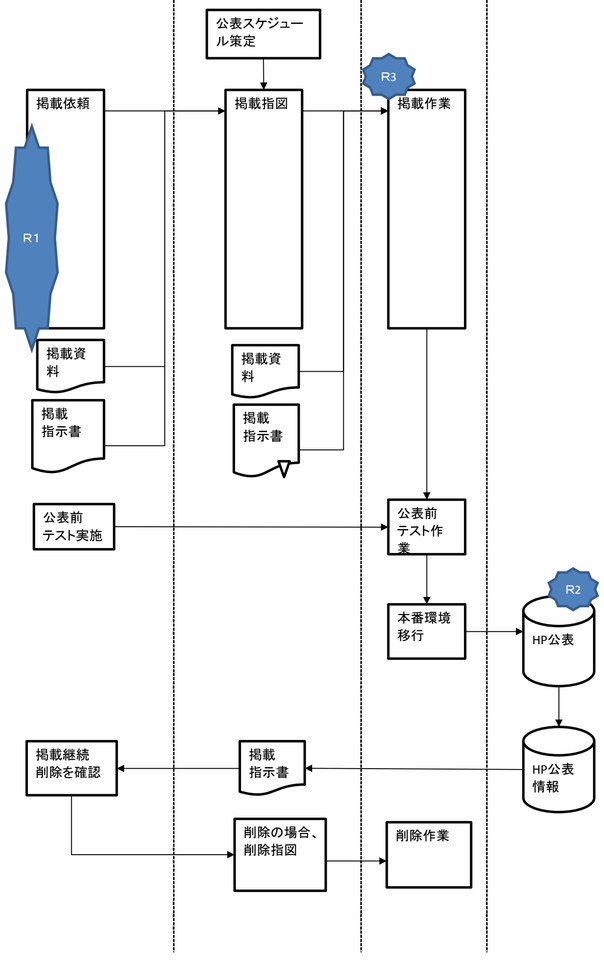
リスク項番	業務リスク（大項目）
1、2	・中期目標期間において各資産ごとのベンチマーク収益率が確保できないリスク。
3a、3b	・基本ポートフォリオとの乖離許容幅を超えるリスク。
4	・年金積立金の管理・運用にあたり、的確なリスク管理又はリスク分析が実施できないことにより、リターン・リスク等の特性が異なる複数の資産に分散投資が行われないリスク。
5、6、7	・ガイドラインが適切に作成されない、又は運用が遵守されないリスク。非伝統的資産の管理が適切に実施されないリスク
8、9	・ベンチマーク収益率が確保できないリスク。
10	・運用対象の多様化が進まないリスク
11	・ESG投資が行えないリスク。
12	・情報の公開するタイミングが遅延すること又は、誤った情報を公開することによる市場への影響や国民に対する透明性や信用性の低下。
13a、b、c、d	・基本ポートフォリオの検証を行わないリスク。
14	・専門家の注意義務及び忠実義務を遵守しないリスク。
15、16、17	・市場の状況を配慮しない資金の投入や回収を行うリスク。
18	・給付に必要な流動性を確保できないリスク。
19	・専門的な人材が確保できないことによる、法人全体の専門性が向上しないリスク。

リスク項番	業務リスク（大項目）
20	・調査研究によって得る、有用な知識を活用できないリスク
21	・研究内容が漏えいするリスク
22	・給与水準を含め法人全体の各経費について効率化に取り組まないリスク。 ・経費執行のモニタリングが不十分なため、予算超過支出を承認するリスク
23	・ICTの整備等に伴い、情報セキュリティで新たに対応すべき事項につき、十分な検討を行わないことにより、情報セキュリティ対策に漏れが生じるリスク
24	・ガバナンス体制が強化されないことによるGPIFの業務の適正化が計れないリスク
25	・体制が整備されないことによる監事機能が発揮できないリスク
26	・情報セキュリティ対策が適切に実施されないリスク
27	・適切な人事評価制度、人員配置計画、採用制度、研修制度を設けていないため、必要な人的資源を確保できず、業務実施を阻害するリスク
28	・災害等により業務が実施できなくなるリスク
29	・感染症の拡大により業務が実施できなくなるリスク
30	・決算作業における様々な事務リスク
31	・外国からの文書（外国税務当局、契約先及び加入国際団体等からの外国語による書類など）が担当者に正しく回付されないことに伴うリスク

（参考３）現状の業務フロー図　抜粋

部・課・係	企画課及び各室課
プロセス名	HP公表
整備状況評価日	
整備状況評価者	
運用評価実施日	
運用評価実施者	



業務記述			業務フロー
No	業務ステップ	業務手続	各室課 / 企画課 / HP掲載委託業者 / GPIF　HP
		GPIFは、情報公開について、「財務情報を含む法人情報のホームページ等での公開に関する規程」を定め、法令等により公開が義務付けられている情報に関する基本規程を設けている。 　さらに、当該規程は、GPIFの業務について透明性を確保し、もしくは、説明責任を果たすために公開する情報、または、GPIFとして広く周知する情報の公開に関する基本規程である。 　また、部・課別に公表する情報、情報公開根拠法令等、公開開始時期、公開終了時期、情報公開の方法など詳細事項については、「財務情報を含む法人情報のホームページ等での公開に関する規程細則」を設定し定めている。 組織規程において、広報は企画課の所掌であり、ホームページ(HP)への情報掲載は企画課が管理している。	
1	情報公表計画	企画課は、HPにおける定期的な情報公開について公表スケジュールを立案する。	
2	掲載依頼	各課・室は、法令等により公表する情報、あるいは、調達情報など周知する情報についてHPに掲載する場合は、企画課に掲載を依頼する。 掲載依頼する課は、掲載指示書、掲載資料を作成し企画課に提出する。 掲載指示書には、掲載情報、掲載期間を明示している(削除時期を特定)。	
3	掲載指図	企画課は、当該掲載指示書を基に、HP掲載委託業者にHP掲載作業を発注する。 掲載情報は掲載依頼する課の責任で作成する。	
4	公表前テスト	HP掲載委託業者は、発注指図に従い、公表日前にHPテスト環境で、HP掲載のテストを実施を企画課に依頼する。 企画課は掲載依頼課にテスト実施を連絡、掲載依頼課がHP掲載する情報の内容物、掲載状況(リンク等)を確認し、テスト合否を判定する。	
5	公表	HP掲載委託業者は、テスト合格後、GPIFのHP本番環境において公表作業を実施、公表開始日にHP掲載する情報開示を行う。	
6	HP公表情報の棚卸	企画課は、HP公表情報について、公表期限超過していないか棚卸する。 企画課は、掲載指示書を用いてHP公表情報の公開期限を確認し、公表要否を掲載依頼課に確認する。掲載依頼課が公表継続・削除を指図に基づき、企画課は、削除作業をHP掲載委託業者に指図し、HP掲載業者はホームページから削除する。	

リスク評価									
リスク概要		リスク対応前（平成29年9月1日）		リスク項番	リスク対応の方針				リスク対応（追加的に発生したリスクを含む）
リスクNo.	リスクの内容	発生頻度	影響度		No.	リスク対応の方針	確認者	確認頻度	
R1	・財務諸表や業務概況書、調達等の内容が誤って公表される。	多	大	12	C1-1 C1-2	・調達案件について、チェックシートを用いるなどして、無理のない公告期間の設定や、詳細な調達内容等の手続きを確認する。 ・掲載資料は掲載依頼する所管課内で複数人によるチェックを行うなど正確性等を検証する。	各課長、室長、副室長 各課長、室長、副室長	（案件発生の都度） （案件発生の都度）	対応策に沿った対応を実施した。リスクの発生は認められない。 【運用管理室】 ・契約継続のための期限延長手続きがなされたものの、契約一覧表の更新に遺漏があった。 対応策：①契約一覧表を契約継続の都度記入する　②契約決裁の都度契約一覧表を添付する。
R2	・法令や規程に基づいて公表が求められている財務諸表等について、公表時期を失念する、又は公表期間を過ぎてもHPに掲載している。	多	大	12	C2	・予め情報公開スケジュールを策定するほか、企画課よりHP掲載にかかる掲載漏れ若しくは掲載終了の確認を四半期ごとに確認を行う。 ・運用委員会議事録簿において掲載期日等の管理を行う。	企画課長	四半期	対応策に沿った対応を実施した。リスクの発生は認められない。
R3	・HPの運用管理は外部業者への委託業務となっているため、緊急掲載等への対応が遅れる。	多	大	12	C3	・ツイッターにより速やかに情報を発信するとともに、委託業者に対し、緊急のHP掲載の臨時作業を依頼する。	企画課長	日次	対応策に沿った対応を実施した。リスクの発生は認められない。

情報セキュリティ管理規程

平成24年規程第１号
平成24年９月６日制定
平成25年６月26日改正
平成26年７月31日改正
平成27年３月23日改正
平成28年10月28日改正
平成29年３月27日改正

第１章　目的及び対象

（目的）

第１条　この規程は、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。）の情報漏えいの防止等情報セキュリティを確保するため、管理運用法人のとるべき対策の枠組みを定め、管理運用法人が自らの責任において対策を図るための措置を講ずることにより、もって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、管理運用法人の管理対象である情報及び情報システムを取り扱う管理運用法人の役員及び職員（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指針

（リスク評価と対策）

第３条　管理運用法人は、その組織の目的等を踏まえ、第10条に定める自己点検の結果、第11条に定める監査の結果、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。

２　管理運用法人は、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。

（情報セキュリティ関係規程の整備）

第４条　管理運用法人は政府機関の情報セキュリティ対策のための統一規範（平成28年８月31日サイバーセキュリティ戦略本部決定）、政府機関等の情報セキュリティ対策の運用等に関する指針（平成28年８月31日サイバーセキュリティ戦略本部決定）及び政府機関の情報セキュリティ対策

のための統一基準（以下「統一規範等」という。）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情報セキュリティに関係する規程及び手順書等（以下「関係規程」という。）を定めるものとする。

２　管理運用法人は、前条第１項の評価結果を踏まえ、関係規程の評価及び見直しを行うものとする。

第３章　情報セキュリティ対策のための基本対策

（管理体制）

第５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　管理運用法人は、最高情報セキュリティ責任者を置く。

３　最高情報セキュリティ責任者は、この規程で規定した情報セキュリティ対策に関する事務を統括し、役員等に対して、別表に掲げる情報セキュリティ対策を講じさせるとともに、その責任を負う。

４　最高情報セキュリティ責任者は、自らの担務を関係規程に定める責任者及び管理者に担わせることができる。

５　管理運用法人は、関係規程の策定等を行う機能を持つ組織として情報セキュリティ委員会を設置し、委員長及び委員を置く。

（対策推進計画）

第６条　最高情報セキュリティ責任者は、第３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。）を定めるものとする。

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。

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うものとする。

（例外措置）

第７条　管理運用法人は、関係規程に定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を関係規程の中で定めるものとする。

（教育）

第８条　管理運用法人は、役員等が自覚をもって関係規程に定められた情報セキュリティ対策を実施するよう、情報セキュリティを含めた情報リテラシー確保のための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（JIS Q27000:2014における情報セキュリティインシデントをいう。以下同じ。）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者は、関係規程に定める報告窓口に連絡するものとする。

３　関係規程に定める責任者は、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、必要な措置を講ずるものとする。

（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。

（監査）

第11条　管理運用法人は、関係規程が統一規範等に準拠し、かつ実際の運用が関係規程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。

（情報の格付）

第12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13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、外部機関との情報の提供、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14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15条　管理運用法人は、管理運用法人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16条　管理運用法人は、情報処理に係る業務を外部委託する場合には、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、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　管理運用法人は、要機密情報を約款による外部サービスを利用して取り扱わないものとする。

４　管理運用法人は、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17条　管理運用法人は、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。

（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18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。

２　管理運用法人は、情報システムの脆弱性対策、アクセスログの定期的点検など情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段を確保するものとする。

（情報システムの運用継続計画）

第19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（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　管理運用法人は、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20条　管理運用法人は、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情報の授受）

第21条　管理運用法人は、インターネット等を用いて情報の授受をする際には、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22条　管理運用法人は、情報システムの利用に際して、役員等に情報セキュリティを確保するために行わせる必要な措置を定め、実施するものとする。

２　管理運用法人は、役員等による規定の遵守を支援する機能について、情報セキュリティリスク及び業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築するものとする。

（関係規程への委任）

第23条　この規程に定めるもののほか、この規程の実施のための手続その他その執行について必要な事項は、関係規程で定める。

附　則

１　この規程は、平成24年９月19日より施行する。

２　情報セキュリティ対策に関する基準（平成21年規程第１号）及び情報セキュリティ対策に関する基準実施細則（平成21年細則第１号）は廃止する。

附　則（平25．６．26改正）

この改正は、平成25年６月26日から施行する。

附　則（平26．７．31改正）

この改正は、平成26年７月31日から施行する。

附　則（平27．３．23改正）

この改正は、平成27年４月１日から施行する。

附　則（平28.10.28改正）

この改正は、平成28年10月28日から施行する

附　則（平29.３.27改正）

この改正は、平成29年４月１日から施行する

別表

〔役員等の遵守事項〕

（情報の作成と入手及び利用時の対策）

1　情報を利用等する場合は自らが担当している業務の遂行以外の目的で利用等しないこと。

2　情報の作成や変更時等に格付及び取扱制限を決定及び明示等するとともに、明示された格付及び取扱制限に従って情報を取り扱うこと。

3　ＵＳＢメモリ等の電磁的記録媒体を用いて情報を取り扱う際、定められた手順に従うこと。

（情報の保存時の対策）

4　要機密情報を保存する際は、アクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。

5　要機密情報を含む電磁的記録媒体、書類又は重要な設計書については、施錠ができる書庫・保管庫に保存する等の適切な管理をすること。

（情報の送信又は運搬時の対策）

6　要機密情報を送信又は運搬する場合には、安全確保に留意して送信手段又は運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のため暗号化等適切な措置を講じること。

（情報のバックアップ）

7　業務に係る情報の滅失等が、業務の遂行に影響を与える可能性が高いと判断される場合、適切な頻度でバックアップ又は複写を取得すること。

（情報の提供時の対策）

8　要機密情報を管理運用法人外に提供する場合は、手順に従い、第５条第４項に規定した責任者に許可又は届出を行うこと。

9　電磁的記録を公表又は提供する場合は、ファイルのプロパティ等に含まれる作成者名、組織名、作成履歴等、公表に不要な付加情報を削除する等、不用意な情報漏えいを防止するための措置を講じること。

10　情報を提供する場合は、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講じること。

（情報の消去時の対策）

11　電磁的記録媒体に保存された情報が不要となった場合は、速やかに情報を消去すること。

12　電磁的記録媒体や書面を廃棄する場合は、全ての情報を復元できないように抹消すること。

（管理運用法人支給以外の端末の利用時の対策）

13　管理運用法人支給以外の端末により情報処理を行う場合は、情報の格付に従い、第５条第４項に規定した責任者に許可又は届出を行うこと。

14　管理運用法人支給以外の端末により情報処理を行う場合は、定められた手続及び安全管理措置に関する規定に従うこと。

（管理運用法人外の情報セキュリティ水準の低下を招く行為の防止）

15　国民等、管理運用法人外の情報セキュリティ水準の低下を招く行為の防止に関する規定に従うこと。

16　国民等、管理運用法人外の者に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、「.go.jp」で終わるドメイン名を使用すること。

（不正プログラム感染及び拡大の防止）

17　不正プログラムの感染防止のため以下の行為を行わないこと。

・安全性が確実ではないファイルをダウンロードする。

・安全性が確実ではないファイルを移送、提供等する。

・安全性が確実ではないファイルを開き、あるいは実行する。

18　不正プログラムに感染した恐れがある場合には、当該端末の通信回線への接続を速やかに切断し、第５条第４項に規定した責任者等に連絡し、その指示に従うこと。

（識別コード又は主体認証情報等の管理）

19　主体認証情報（パスワード等）の管理に当たって、「他者に知られない」「他者に教えない」「忘れない」「容易に推測可能なものを用いない」「定期的に更新する」ことを徹底すること。

20　主体認証情報格納装置（IC カード等）の管理に当たって、「他者に貸与しない」「紛失しない」こと。

21　識別コード（ユーザID 等）が不要になった場合又は主体認証情報が他者に使用された（又は使用される危険性が生じた）場合には、速やかに第５条第４項に規定した管理者に届け出ること。

（端末の利用時の対策）

22　モバイル端末を利用する際、第５条第４項に規定した責任者の承認を得るとともに、定められた手順に従い適切に利用すること。

23　端末は業務目的のみで使用し、その際使用する端末において利用可能と定められたソフトウェアのみを利用すること。

（通信回線の利用時の対策）

24　許可されていない端末等を通信回線に接続せず、許可された通信回線のみを利用すること。

（電子メールの利用時の対策）

25　要機密情報を含む電子メールを送受信する場合には、第５条第４項に規定した責任者が指定（管理運用法人によって運営又は外部委託されているものをいう。）した電子メールサービスを利用すること。

（ウェブの利用時の対策）

26　ウェブブラウザのセキュリティ設定を適切に行うこと。（あらかじめ第５条第４項に規定した管理者が設定している場合には、それに従って適切に使用すること。）

27　ウェブサイトに要機密情報を入力して送信する場合は、次の事項を確認すること。

(a)送信内容が暗号化されていること。（ウェブブラウザの鍵アイコン表示等による確認）

(b)送信先が想定している組織のウェブサイト（サイト証明書等による確認）

（兼務の禁止）

28　情報セキュリティについての責任者（又はその上司）の立場にあって、情報セキュリティに関する申請を自らが行う場合には、自分以外の適切な承認権限者に申請すること。

（違反への対処）

29　情報セキュリティ関係規程への重大な違反を知った場合は、速やかに第５条第４項に規定した責任者にその旨を報告すること。

（例外措置の運用）

30　定められた審査手続きに従い、許可権限者に規定の例外措置の適用を申請すること。

（情報セキュリティ対策の教育）

31　情報セキュリティ対策についての教育を、年に一度は受講すること。ただし、人事異動等により新しい職務等に着任した場合には、必要に応じて受講すること。

（自己点検）

32　計画に基づき決定された自己点検票及び手順に従い、自己点検を実施すること。

（情報セキュリティインシデントの対処）

33　不審メールの受信等情報セキュリティインシデントの可能性を認知した場合は、速やかに報告窓口及び第５条第４項に規定した責任者に連絡するとともに対処手順等に従いその対処に努めること。

（外部委託における対策）

34　委託先に要機密情報を提供する場合は、提供する情報を必要最小限とし、委託先において情報が不要になった場合、あるいは外部委託終了時には委託先に不要な情報を返却、廃棄又は抹消をさせること。

35　委託先における情報セキュリティインシデントを認知した場合は、速やかに報告窓口及び第５条第４項に規定した責任者又は管理者に連絡するとともに対処手順等に従いその対処に努めること。

（約款による外部サービスの利用における対策）

36　利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

（情報セキュリティ関係規程の運用）

37　情報セキュリティ関係規程に係る課題及び問題点を発見した場合は、第５条第４項に規定した責任者又は管理者を通じて統括情報セキュリティ責任者に報告すること。

内部統制に関する規程

平成27年規程第３号
平成27年３月30日制定
平成27年５月９日改正
平成27年８月１日改正
平成28年５月31日改正
平成29年９月29日改正

第１章　総則

（目的）

第１条　この規程は、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。）における内部統制の推進体制の整備等に関し、必要な事項を定めることを目的とする。

（内部統制の基本方針）

第２条　理事長は、中期目標及び中期計画に基づき法令等を遵守しつつ業務を行い、管理運用法人の使命を有効かつ効率的に果たすため、内部統制の推進体制の整備等に関する基本的な方針(以下「内部統制の基本方針」という。）を策定する。

第２章　推進体制

（内部統制担当役員）

第３条　内部統制の推進体制の整備等を担当する役員(以下「内部統制担当役員」という。）は、理事（総務・企画等担当）とする。

２　内部統制担当役員は、次の各号に掲げる事務を行うものとする。

(1) 内部統制の推進に関する事務を統括すること

(2) 内部統制の推進体制を整備すること

(3) 管理運用法人の役員（経営委員会の委員長及び委員を除く。）、参与及び職員（以下「役員等」という。）における法令等の遵守状況を把握すること

(4) 役員等に内部統制の推進に関して必要な研修を行うこと

(5) 役員等からの内部統制の推進に関する質問又は相談を受けること

(6) その他内部統制の推進に関して必要な調整を行うこと

（総括内部統制推進責任者）

第４条　管理運用法人に、総括内部統制推進責任者を置く。

２　総括内部統制推進責任者は、コンプライアンス・オフィサーをもって充てる。

３　総括内部統制推進責任者は、内部統制担当役員を補佐し、内部統制推進責任者の統括その他内部統制の推進体制の整備等に関する事務を行うものとする。

４　管理運用法人における内部統制の推進体制の整備等に関する部門(以下「内部統制推進部門」という。）は、企画部企画課とする。

（内部統制推進責任者）

第５条　管理運用法人は、総括内部統制推進責任者の事務を分掌する者として、内部統制推進責任者を置く。

２　内部統制推進責任者は、部、室及び事務室の長をもって充てる。

３　内部統制推進責任者は、所管する部、室及び事務室における内部統制の推進に関する事務を統括するものとする。

（内部統制推進管理者）

第６条　管理運用法人は、総括内部統制推進責任者の事務を分掌する者として、内部統制推進管理者を置く。

２　内部統制推進管理者は、室長、事務室長及び課長をもって充てる。

３　内部統制推進管理者は、所管する室、事務室及び課における内部統制の推進に関する事務を行うものとする。

第３章　内部統制委員会

（内部統制委員会）
第７条　管理運用法人に、内部統制の推進を図るため、内部統制委員会を設置する。
２　内部統制委員会の委員は、理事長、理事、上席審議役、審議役、総括内部統制推進責任者、リーガル・オフィサー、内部統制推進責任者及び次長とし、委員長は理事長をもって充てる。
３　委員長に事故があるときは、理事（総務・企画等担当）がその職務を代理する。
４　委員長は、必要に応じ、説明及び報告を求め、又は事情を聴取するために、委員以外の者に出席を求めることができる。
５　委員長は、必要に応じ、委員以外の者を出席させ、意見を述べさせることができる。
６　内部統制委員会は、理事長が招集する。
７　内部統制委員会は、次の各号に掲げる事項を審議する。
(1) 内部統制の基本方針に関する事項
(2) 業務実施の障害となるリスク（以下「業務リスク」という。）の識別、分析及び評価並びに当該リスクへの適切な対応を図るための次に掲げる事項
　イ　部、室及び事務室ごとの業務フロー図の作成
　ロ　業務フローごとに内在する業務リスク因子の把握及び業務リスク発生要因の分析
　ハ　把握した業務リスクに関する評価
　ニ　業務リスク顕在時における対応方針、広報方針及び体制の策定
(3) 業務リスクの防止に係る啓発に関する事項
(4) 部、室及び事務室の業務リスクに係る総合的な調整に関する事項
(5) 事故・災害等の緊急時に関する次に掲げる事項
　イ　防災業務計画及び事業継続計画(ＢＣＰ)の策定及び計画に基づく訓練等の実施
　ロ　事故・災害時の対策本部の設置、構成員の決定
　ハ　事故・災害時の初動体制の構築及び情報収集の迅速な実施
(6) この規程及び制裁規程の制定又は変更に関する事項
(7) コンプライアンスの推進に関すること
(8) 違反行為等の再発防止策に関すること
(9) 反社会的勢力への対応方針等に関すること
(10) 前各号に掲げるもののほか、内部統制の推進に関し必要な事項
８　内部統制委員会の庶務は、企画部企画課において行う。
（内部統制担当役員による報告）
第８条　内部統制担当役員は、次に掲げる事項について、定期的に内部統制委員会に報告するものとする。
(1) 内部統制担当役員、内部統制推進部門及び総括内部統制推進責任者間の報告会の実施状況
(2) 内部統制担当役員と職員との面談の実施状況
(3) 内部統制担当役員によるモニタリング体制の運用状況
(4) 内部統制推進部門におけるモニタリング体制の運用状況
(5) 研修会の実施状況
２　内部統制委員会は、前項の報告を受け、必要があると認めたときは、改善策を検討するものとする。

第４章　コンプライアンス委員会

（コンプライアンス委員会）
第９条　内部統制委員会の下に、コンプライアンスに関する事項について審議するため、コンプライアンス委員会を設置する。
２　コンプライアンス委員会の委員は、理事長、理事、上席審議役、審議役、総括内部統制推進責任者、リーガル・オフィサー、総務部長及び理事長が任命する外部委員（法務に関する有識者である第三者）とし、委員長は理事長をもって充てる。
３　委員長に事故があるときは、理事（総務・企画等担当）がその職務を代理する。
４　委員長は、必要に応じ、説明及び報告を求め、又は事情を聴取するために、委員以外の者に出席を求めることができる。

５　委員長は、必要に応じ、委員以外の者を出席させ、意見を述べさせることができる。
６　コンプライアンス委員会は、理事長が招集する。
７　コンプライアンス委員会は、内部統制委員会が審議する事項のうち、第7条第7項第7号から第9号までに掲げる事項その他コンプライアンス委員会が必要と認めた事項を審議する。
８　コンプライアンス委員会は、前項に規定する事項について審議を行うために、必要な調査を行うことができる。また、管理運用法人内部に設置されている各種委員会及び内部通報及び外部通報の相談窓口に必要な情報の提供を求めることができる。
９　コンプライアンス委員会は、必要があると認めるときは、所管部署に対して審議等の結果に基づく意見・提言を行うことができる。
１０　コンプライアンス委員会の庶務は、企画部企画課において行う。
（コンプライアンス・オフィサーによる報告）
第10条　コンプライアンス・オフィサーは、役員等における法令遵守等の状況を確認し、これをコンプライアンス委員会に報告するものとする。

附　則
この規程は、平成27年４月１日から施行する。
附　則（平27.５.９改正）
この改正は、平成 27 年５月９日から施行する。
附　則（平27.８.１改正）
この改正は、平成 27 年８月１日から施行する。
附　則（平 28 年５.31 改正）
この改正は、平成 28 年５月 31 日から施行する。
附　則（平成 29. ９.29 改正）
この改正は、平成 29 年 10 月１日から施行する。

業務リスクの識別、分析、評価に関する細則を次のように制定する。

平成 29 年細則第 1 号
平成 29 年 3 月 31 日制定
理事長　髙橋則広

業務リスクの識別、分析、評価に関する細則

内部統制に関する規程第７条第７項（２）に規定する業務実施の障害となるリスクの識別、分析及び評価については、様式第１号から第３号までにより行うものとする。

様式第１号

様式第２号

様式第３号

附則
この細則は、平成 29 年 4 月 1 日から施行する。