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

第１章　基本方針等

（基本方針）

第１条　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。）は、情報漏えいの防止等情報セキュリティを確保するため、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。）、公文書等の管理に関する法律（平成21年法律第66号）、管理運用法人の内部統制の基本方針等を踏まえ、情報セキュリティ対策の目標、基本対策等を策定し、情報セキュリティ水準の向上を図ることとする。加えて、情報セキュリティに関係する規程、細則及び手順書等（以下「関係規程等」という。）に定められた事項及び対策を実行の上、評価し、必要に応じて見直すというPDCA(Plan・Do・Check・Act)サイクルを実施する。

（情報セキュリティ対策の目標）

第１条の２　管理運用法人は、第２項に掲げる管理運用法人内外からの情報資産に対する脅威（以下「脅威」という。）に対処するため、管理運用法人が被る損害又は外部に与える損害を最小限にくい止めることにより、管理運用法人の業務の継続に甚大な悪影響を及ぼす事態を起こさないことを目標として情報セキュリティ対策を講ずるものとする。

２　管理運用法人が情報セキュリティ対策において対処する脅威は、次に掲げるとおりとする。

（１）外部からの意図的な攻撃（不正侵入、コンピュータウイルス、盗聴、盗難、改ざん、破壊、消去、漏えい等）

（２）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。）による意図的な不正使用等（不正使用、改ざん、破壊、消去、漏えい、持出し等）

（３）非意図的要因（ただし、ハードウェア障害、ソフトウェア障害、ネットワーク障害、設備の故障、非意図的な誤使用等を除く。）

（４）災害（落雷、火災、水害、地震等）

（５）管理運用法人の情報資産を用いた外部への意図的・非意図的な加害行為（コンピュータウイルスの送信、不正侵入等）

（目的）

第１条の３　この規程は、第１条に基づき、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。

（用語の定義）

第１条の４　この規程における用語を以下のとおり定義する。

２　「情報」とは、以下の（１）から（４）までに掲げるものをいう。

（１）役員等が職務上使用することを目的として管理運用法人が調達し、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（以下「外部媒体等」という。）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。）

（２）その他の情報システム又は外部媒体等に記録された情報（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、役員等が職務上取り扱う情報

（３）（１）及び（２）のほか、管理運用法人が調達し、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

（４）文書管理規程第２条第１号に規定する法人文書

３　「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、管理運用法人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。

４　「情報セキュリティ」とは、情報の機密性、完全性及び可用性をいう。

５　「情報セキュリティ対策」とは、情報セキュリティを確保するために必要な措置をいう。

６　「統一基準群」とは、以下の（１）から（４）までに掲げるものをいう。

（１）政府機関等のサイバーセキュリティ対策のための統一規範

（２）政府機関等のサイバーセキュリティ対策の運用等に関する指針

（３）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

（４）政府機関等の対策基準策定のためのガイドライン

７　「情報セキュリティインシデント」とは、JIS Q 27000:2019における情報セキュリティインシデント（望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの）をいう。

８　「情報セキュリティ要件」とは、アクセス制御等情報セキュリティを確保するために、情報システムにおいて必要となるセキュリティ機能をいう。

９　「情報資産」とは、情報及び情報を管理する仕組み（情報システム、事務室、保管庫及びその他情報を保管するための施設設備（情報システムを除く。））の総称をいう。

10　「機密性」とは、情報に関して、認可さ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。

11　「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。
12　「可用性」とは、情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。
13　「情報リテラシー」とは、電子計算機及び通信回線等を活用して情報を扱うための基本的な知識及び能力（情報セキュリティに関するものも含む。）をいう。

（適用対象）
第２条　この規程の適用対象とする者は、役員等とする。
２　削除

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、サイバーセキュリティ基本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。

（関係規程等の整備）
第４条　管理運用法人は統一基準群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関係規程等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、関係規程等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　削除
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等に定める責任者及び管理者に担わせることができる。

５　削除

（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、関係規程等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等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等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、関係規程等に定める報告窓口に連絡するものとする。

３　関係規程等に定める責任者は、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。

（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、外部委託を実施する際に要機密情報を取り扱う場合は、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、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。

（情報セキュリティ要件の明確化に基づく対策）

第23条　管理運用法人は、アクセス制御の観点など導入すべきセキュリティ機能及び主要な脅威を防ぐための情報セキュリティ要件を明確化するとともに、当該要件を確保する。

（情報システムの構成要素についての対策）

第24条　管理運用法人は、電子計算機及び通信回線等、個別の情報システムの構成要素について、その特性及びライフサイクルに応じて必要な対策を実施する。

（関係細則への委任）

第25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、理事長が別に定める。

２　この規程の適用に際し、理事長は必要な経過措置等を定めることができる。

（規程の制定又は改廃）

第26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。

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　関係規程等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。

（業務委託における対策）

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、あるいは業務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。

（要機密情報を取り扱う場合の外部サービスの利用における対策）

36　要機密情報を取り扱う場合の外部サービスの利用に関する規定を整備すること。

（要機密情報を取り扱わない場合の外部サービスの利用における対策）

37　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要機密情報を取り扱わない場合の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。

（関係規程等の運用）

38　関係規程等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。