平成 30 年 4 月 26 日
最高情報セキュリティ責任者

平成 30 年度情報セキュリティ対策を総合的に推進するための計画

情報セキュリティ管理規程第 6 条第 1 項に基づき、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。）を以下のとおり定める。

１．法人業務及び取り扱う情報

法人業務は、厚生年金保険法及び国民年金法の規定に基づき厚生労働大臣から寄託された積立金の管理及び運用を行い、その収益を国庫に納付することにより厚生年金保険事業及び国民年金事業の運営の安定に資することを目的としている。よって、法人が取り扱う情報は、国の行政運営上重要なものを多く含み、外部への情報漏洩や改竄、消失等が発生した場合には、極めて重大な結果を招く恐れがある。

２．平成 29 年度情報セキュリティ対策の実施状況・評価及び課題

別紙「平成 29 年度対策推進計画の実施状況・評価及び課題」を参照。

３．平成 30 年度の情報セキュリティ対策

上記２の評価等を踏まえ、（１）人的対策及び（２）技術的対策の観点から、以下の情報セキュリティ対策に取り組むこととする。

なお、人的対策における対象者は、派遣職員等を含む全ての役職員とする。

（１） 人的対策

ア．最高情報セキュリティアドバイザーの設置

法人に最高情報セキュリティアドバイザーを設置する。（調達予定時期：上期）

イ．情報セキュリティに関する教育・訓練

（ａ）e-Learning を用いた研修（実施予定時期：下期）

昨年度に引き続き、e-Learning を用いた研修を実施する。

（ｂ）集合研修（実施予定時期：上期）

標的型攻撃メール訓練や自己点検等における評価結果や監査室監査の結果、セキュリティ関係規程の改正等を踏まえ、遵守すべき手順等に関する周知・徹底を目的とした研修を行う。また、今年度も役職員向け研修に加えて、情報セキュリティ責任者等を対象とした研修を実施する。なお、集合研修は、引き続き外部講師を招いての実施を検討する。

（ｃ）標的型攻撃メール訓練（実施予定時期：随時）

昨年度から新たにビジネスメール詐欺（ＢＥＣ）が企業にとり大きな脅威となっており、インシデント対応手順の周知や初動対応の徹底等を目的にして、引き続き標的型攻撃メール訓練を通期にわたり分散して実施する。本訓練実施業務に

ついては、ネットワークシステム運用委託業者がインフラを提供し、情報管理セキュリティ対策課がコンテンツを作成し実施する。

（ｄ）注意喚起（通年）

不審メールの受信等情報セキュリティ脅威の発生時等にタイムリーな注意喚起を行い、役職員の情報セキュリティ意識の醸成を図る。

（ｅ）ＣＳＩＲＴ職員に対する研修等（実施予定時期：下期）

ＣＳＩＲＴに属する職員に対して必要な研修を行う。また、厚生労働省との共同訓練実施等も考慮した上でＣＳＩＲＴに係る訓練を検討する。（訓練については研修実施後を予定。）

なお、ＮＩＳＣ等が主催するＣＳＩＲＴ研修やＣＹＤＥＲ等の研修については、ＣＳＩＲＴ構成員を積極的に参加させる。

（ｆ）セキュリティ人材の育成に係る研修（実施予定時期：通年）

昨今の情報セキュリティを取り巻く環境の複雑化・高度化を踏まえ、サイバー攻撃等のインシデントに備えることを目的とし、外部専門機関等の活用も含め、職員の対処能力等の向上を目的とした研修等に参加する。

ウ．情報セキュリティ対策の自己点検（実施予定時期：上期）

昨年度の結果等を踏まえ自己点検計画を策定し、自己点検を実施する。

エ．運用受託機関等の情報セキュリティ管理

運用受託機関等の情報セキュリティ管理体制に関する平成 29 年度評価結果について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とともに、評価結果を踏まえた対応を検討する。

また、各室課は「運用受託機関等における情報セキュリティ対策実施規程」等に従い、運用受託機関等が実施する情報セキュリティ対策の履行状況の確認等を通じて年度末のセキュリティ評価を実施する。

履行状況の確認等を行う際は、運用受託機関等に対して、必要に応じ各室課と同行し実地検査を行う。

（２）技術的対策

昨年度の課題等を踏まえ、以下の技術的対策を実施する。

ア．セキュリティ診断結果を踏まえた対策

昨年度実施したネットワークシステムにおけるセキュリティ診断結果を踏まえた対策を検討、実施する。今年度のセキュリティ診断（含むペネトレーションテスト）については、外部の診断業者を調達の上、下期に実施する。

イ．厚生労働省が予定しているマネジメント監査等（自己点検、標的型攻撃メール訓練、ペネトレーションテストを含む）については、現時点で実施内容は未定であるが、指摘事項等が発見された場合は、指示に従い対応する。

（３）その他

ア．情報セキュリティ関係規程の改正（実施予定時期：平成 30 年度政府統一基準群

の改正以降）

平成 30 年度における政府統一基準群の改正（夏以降に予定されている）を踏まえて法人の情報セキュリティ関係規程の改正を行う。

イ．法人ネットワークの更改に向けた情報セキュリティ対策の各種実装（機能・仕様等）について検討する。

ウ．ＩＰＡマネジメント監査のフォローアップ（実施時期未定）について、必要に応じて対応する。

４．情報セキュリティ監査

平成 29 年度に引き続き、監査室が下期に実施を予定している情報セキュリティ対策にかかる第三者によるマネジメント監査について、監査結果を踏まえ必要な対策を検討する。

以上