情報セキュリティ強化等に向けた組織・業務改革

－日本年金機構への不正アクセスによる情報流出事案を踏まえて－

平成27年９月18日

厚生労働省

第１　日本年金機構における情報流出事案に関する総括

今回の事案についての主な反省点

１．情報セキュリティの重要性に関する意識の欠如

○膨大な個人情報や機微な情報を扱っている組織であるにもかかわらず、情報セキュリティ対策の重要性に関する意識が省全体として希薄。その結果、事前の人的体制と技術的な対応、適切な情報共有が不十分。
○機構を監督する厚労省自身の長きにわたっての意識の欠如が、機構の個人情報流出につながった大きな要因。

２．組織的な危機管理対応の欠如

○事案発生後、「事案が収束してから書面で上司に報告する」「自分は単なる窓口」といった認識などから、職員間、上司と部下、関係組織間で情報や危機感が適時に共有されず、組織が一体として危機に当たることができなかった。
○今回の事案が発生するまで、業務運営におけるリスクの所在や評価等について組織的に把握、評価されていなかった。

３．組織横断的、有機的な連携の欠如

（1）4月22日の標的型攻撃についての厚労省の対応

○5月8日攻撃では、省内幹部に情報共有が行われず、省全体として適時適切な対応ができなかった。情報共有が適切になされていれば、4月22日攻撃との共通性も含め、省、機構を通じて、危機意識が醸成され、その後の対応が異なるものとなった可能性。
○相互の意思疎通や組織横断的、有機的な連携を図り、厚労省の組織全体として一丸となった対応が重要。

（2）厚労省と機構の関係

○厚労省と機構の間の情報共有が不十分。政府管掌年金事業の運営は厚労省と機構が車の両輪となって共に担う、との考え方を再確認し、厚労省による機構の監督や機構との連携のあり方についてゼロベースで点検・再構築。

再発防止に向けた基本的考え方

○以上の反省点を踏まえ、年金局や機構だけでなく、厚労省所管法人等も含めた厚労行政全体について、ガバナンス、組織内、組織間連携、リスク認識の強化に努めていくが、今回の事案に照らし、特に情報セキュリティ対策強化を図る。
○このため、「情報セキュリティ強化等に向けた組織・業務改革推進本部（仮称）」を設置し、以下の具体的取組を実施。

第2　今回の事案を踏まえた再発防止策

1. 厚生労働省における情報セキュリティ対策の強化

組織的対策

○来年度に向け、省内の情報システム、情報セキュリティに関する機能を再編し、情報セキュリティ対策の司令塔機能を強化。それまでの間は、以下の措置を速やかに講じる。
①情報セキュリティ対策の実務部門の強化として、情報セキュリティ対策室（仮称）を設置。
②即応性の向上、権限の強化（予算、人事、業務面）の観点から、CISO（最高情報セキュリティ責任者）及びCSIRT体制（インシデント対応チーム）の見直し。
・CISOを官房長から厚生労働審議官に、CSIRT責任者を官房長から情報政策・政策評価審議官に見直し。
・CSIRT要員として、補佐、係長クラスの職員（事案の対処支援や関係者との連絡調整に従事）を充てる。

人的対策

○毎年、全職員の意識向上を図るための情報セキュリティに対する独自の集中的な取組期間を設定。幹部職員においては、情報セキュリティに関する意識改革のほか、基盤整備等の業務改革、人的資源の確保、配分等のマネジメント面の意識改革を行う。
○標的型メール攻撃に対する危機意識やリテラシー向上のための実践的な訓練の実施。
○情報セキュリティ対策室（仮称）に情報セキュリティに関する外部専門家を常勤で配置。組織内での人材養成方策の検討。
○過去の事案から得られた危機管理に関する教訓や知識の蓄積と継続性の確保。

業務運営対策

○セキュリティポリシーや対処手順書の見直しにより、インシデント発生時の責任者への報告、連絡体制、CSIRTと担当部局の役割、責任等を明確化。
○個人情報等重要情報を取り扱う省内情報システムについて、リスク評価の実施及びその結果に基づく対策。緊急的対応として、インターネットから物理的又は論理的に分離し、インターネット接続端末で利用しないこととする措置を講じた。

技術的対策

○各種ウィルスの侵入を検知する入口対策に加え、不正な通信をリアルタイムに監視し、遮断する機能など標的型攻撃を早期に検知するための内部、出口対策を強化。
○本省及び所管法人等のシステムについて、業務実態やリスク評価を踏まえた設計、運用、組織間連携を含むインシデント対応。
○情報システムの調達において、最新のセキュリティパッチが適用されるよう徹底。

2. 厚生労働省と機構の関係の強化

○政府管掌年金事業の適正な運営は厚生労働省と機構が車の両輪となって共に担う、との考え方を再確認し、ガバナンスや組織風土のゼロベースからの抜本改革などの機構の改革と併せて、厚生労働省による機構への指導監督を強化。
○また、社会保障審議会年金事業管理部会に新たな委員を任命するとともに、事務局へ民間から複数の参与を任命。監視機能を強化した同部会に対する説明責任を果たしつつ、着実に取組。

①機構ＬＡＮシステムについて、年金局事業管理課システム室を中心に取り組むこととし、権限の所在を明確にするとともに、体制を強化。
②機構の改革の取組が着実に進むよう、機構に対するモニタリング、監査を強化。
③機構が業務運営上定める内規等について、年金局の担当部署がチェックし、共有することをルール化。
④事務処理誤りについて、機構から年金局への報告を徹底。
⑤情報共有について、幹部も含めた各レベルでの日常的な報告、連絡、相談のルール化。
⑥年金局と機構の相互の人事交流の拡大、年金事務所での勤務経験を年金局職員のキャリアパスに位置づけ。

○機構の改革の取組が着実に進むようにするため、年金局の体制を強化。

3. 厚生労働省所管法人等に対する監督と情報セキュリティ対策の強化

厚労省所管法人等における情報セキュリティ対策は、当該法人等が責任を持って行うことを基本としつつ、厚労省と当該所管法人等が一体となって、日常的な対策やインシデント発生時などの緊急時の対応を行っていく。

○所管法人等を所管する部局の職員、幹部に対し、情報セキュリティにおける当該法人等との連携に関する教育訓練の実施。
○インシデント発生時における当該法人等と厚労省担当部局の役割の明確化、迅速な情報提供のための連絡窓口の見直し。
○個人情報等重要情報を取り扱うシステムについて、全ての所管法人等を対象としたリスク評価の実施及びその結果に基づく対策。緊急的対応として、インターネットから物理的又は論理的に分離するなど必要なシステム上の措置を講じた。
○所管法人等において、個人情報等の管理状況やルールについて、自己点検を実施。併せて、当該法人等に対し、情報セキュリティ対策室（仮称）がPDCAの観点から監査（助言）。