『情報セキュリティ強化等に向けた組織・業務改革』の進捗状況

資料1

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**。

対応

○ 情報セキュリティ対策室を設置した。（10月1日）

○ 情報セキュリティポリシー・対処手順書等について、**CISO・CSIRT責任者の変更**と、**CSIRT体制・役割の明確化**等の見直しを実施した。（10月1日、12月21日）

○ 情報セキュリティ対策室で、不審メールの受信状況等を収集・集約の上、専門人材（委託業者）の分析能力等を活用し、**サイバー攻撃相互の関連性等を予測し、次の攻撃を想定した指示を発出する**等の対応を適時適切に実施。

人的対策

○ 毎年、情報セキュリティに係る**集中的な取組期間**を設定。幹部職員には、情報セキュリティに関する意識改革のほか、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。

○ 情報セキュリティ対策室に**外部専門家を常勤で配置**。緊急対応時に外部事業者による**専門知識を生かした支援**の実施。

○ 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**。

対応

○ 全職員に重要情報の適正管理について注意喚起し、所管法人等にも周知を実施した。

○ 幹部職員等に**重層的な情報セキュリティ研修**を実施した。幹部職員に**マネジメント研修を実施**した。

○ 情報セキュリティ対策の**外部専門家を公募**した。

○ 過去事案や情報セキュリティの動向を研修教材に反映した。

○ 集中的な**取組期間を「6月」に設定**し、毎年、今回の事案を風化させない取組を実施。

○ 27年度補正予算で、**CSIRTへの緊急・専門的支援業務の外部委託**にかかる経費を計上。

○ インシデント経験者による勉強会形式の研修を実施。

業務運営対策

○ **情報セキュリティポリシーや対処手順書等の見直し**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**と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。

対応

○ 情報セキュリティポリシー・対処手順書等について**インシデント発生時の報告、連絡体制の明確化**等を内容とした見直しを実施した。（12月21日）

○ 27年度補正予算で、厚労省・所管法人等の保有システムの**リスク評価を実施**するための経費を計上。

技術的対策

○ ウイ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**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**調達で最新のセキュリティパッチが適用**されるよう徹底。

対応

○ 情報システムの**調達仕様書作成の手引きの見直し**を実施、**所管独法にも厚労省と同水準の見直し**を周知。（12月）

○ 27年度補正予算及び28年度予算で、標的型攻撃に対する**多重防御の取組**（入口・内部・出口対策）を計上。

○ 27年度補正予算で、厚労省・所管法人等の保有システムの**リスク評価を実施**するための経費を計上。

2. 厚生労働省と機構の関係の強化

監督指導の強化

○ 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**。

対応

○ 機構に**業務改善命令**(9/25)(12/9業務改善計画提出)
○ 下記により機構への**指導監督を強化**した。(10月1日～)
① 機構LAN･インシデント対応等の**責任の所在を年金局システム室に一元化**し、さらに同室の体制を強化。
② 年金局職員が機構に常駐し、会議出席などの**モニタリング**を実施。年金局監査室も機構に常駐し、監査実施。
③ 年金局が、機構の**内規等を事前に確認**。
④ 機構常駐の監査室が、**事務処理誤りを一元的に把握**。
⑤ 機構と年金局のカウンターパートを明確にし、共通様式である進捗管理表により**継続的な課題等を整理・共有**。
○ 年金事業管理部会に委員7名(情報セキュリティ専門家含む)を任命。事務局員に民間から参与2名を任命。

○ 年金事務所などへの**現場実習**の拡大や機構の研修への年金局職員の参加により、年金実務の知識を習得。
○ 年金局システム室に**外部専門家を登用**する。
○ 年金局･機構間のさらなる**人事交流の拡大**を図る。
○ 年金局職員について、原則として年金事務所での勤務経験を課長補佐等への**登用のキャリアパス**とする。

体制強化

○ 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**。

対応

○ 機構LAN･インシデント対応等の責任の所在を年金局システム室に一元化し、**同室の体制を強化**。(10月1日～)

○ 機構の改革実現に向けた支援等を担当する管理職の設置に向け調整中。

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

○ 厚労省所管法人等の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、情報セキュリティ上の**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**するなどシステム上の必要な措置を講じた。
○ 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が監査（助言）。**

対応

○ 所管法人等の**管理職を対象とした研修**を実施。（10月）
○ 所管法人等の幹部を対象とした**情報セキュリティ対策に関する連絡会議**を実施。（12月）
○ 情報セキュリティポリシー・対処手順書等について、**インシデント発生時における所管法人等と厚労省担当部局の役割の明確化**等を内容とした見直しを実施した。（12月21日）

○ 厚労省が行う教育訓練の内容については、適時適切に所管法人等に情報提供。
○ 27年度補正予算で、厚労省・所管法人等の保有システムの**リスク評価の実施、情報セキュリティ監査の実施**にかかる経費を計上。