（2）　日本年金機構情報セキュリティポリシー等に基づいて実施すべき情報セキュリティ対策を事業担当部署に対して周知徹底することなどにより、情報システムの調達、保守等業務の外部委託等において適切な情報セキュリティ対策が講じられるよう改善させたもの

科　　目	業務経費
部　局　等	日本年金機構本部
情報システム名	コールセンター機器群
情報システムの概要	構内電話交換機、統計管理装置（サーバ）等の機器により構成され、コールセンターにおいて電話相談を行うために使用しているシステム
上記システムの調達、運用等に要した費用の額	6億1871万円（令和2年4月～5年10月）

1　日本年金機構における情報セキュリティ対策の概要等

⑴　日本年金機構情報セキュリティポリシーの概要等

日本年金機構（以下「機構」という。）は、年金事業に係る業務を円滑に実施するために、多数の情報システムを開発し、管理し、運用するなどしている。そして、機構は、情報システムについて、適切な情報セキュリティ対策を講じていくことが必要不可欠であるとして、平成22年1月に日本年金機構情報セキュリティポリシー（平成22年規程第16号。以下「ポリシー」という。）を策定している。

ポリシーによれば、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とされている。そして、情報システムごとに当該情報システムを所管する事業担当部署の長を情報システムセキュリティ責任者（以下「セキュリティ責任者」という。）として設置することとされており、セキュリティ責任者は、情報セキュリティ上の脅威に対抗するために必要となるセキュリティ要件(注1)を適切に決定し、仕様書等に明記することとされている。

ポリシーによれば、セキュリティ責任者は、サーバ装置、端末等の設置又は運用開始時に、これらの機器上で使用するソフトウェアに関連して公開されているぜい弱性についての対策（以下「ぜい弱性対策」という。）を実施するとともに、ぜい弱性対策の状況を定期的に確認し、ぜい弱性対策が執られていない状態が確認された場合等には、ぜい弱性対策計画を策定し、必要な措置を講ずることとされている。

また、ポリシーによると、システム企画部長は、セキュリティ責任者が作成した情報資産台帳を利用して、情報システムのセキュリティ要件について管理することとされている。そして、情報資産台帳に登録された情報システムは、令和3年10月時点で719システムとなっている。このうち、他の機器と通信を行っており、ソフトウェアのぜい弱性対策等の情報セキュリティ対策を講ずることが特に重要とされる情報システムは、35システムとなっている。

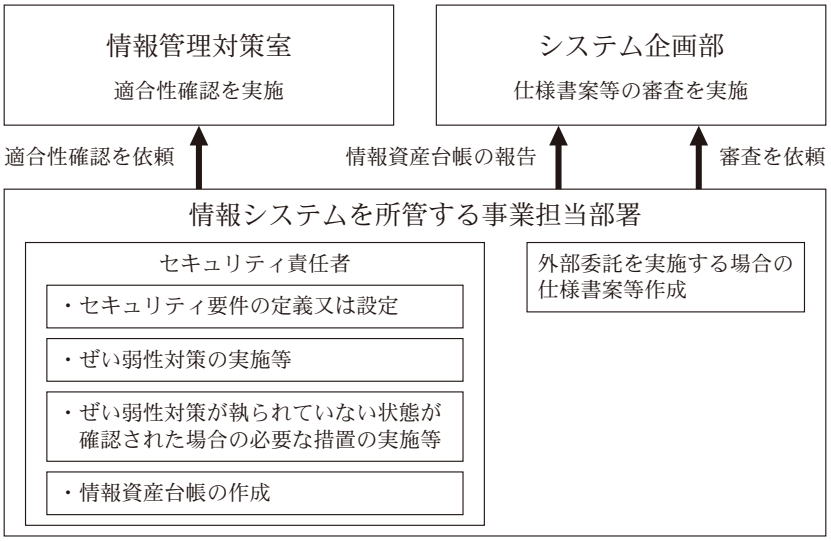
⑵　情報セキュリティ要件確認実施要領等の概要

情報管理対策室は、2年3月に情報セキュリティ要件確認実施要領（令和2年要領第225号。以下「要件確認要領」という。）を制定し、セキュリティ責任者等が定義又は設定を行ったセキュリティ要件がポリシーに適合しているかの確認（以下、この確認を「適合性確認」という。）を実施するための手順等を定めて、同年9月から施行している。要件確認要領によると、事業担当部署において情報システムの新規開発、改修、購入、役務の提供（無償であるものを含む。）、運用等を行おうとする場合、事業担当部署は、セキュリティ要件確定前、調達前等に、情報管理対策室に対して適合性確認の依頼を行って確認を受けることとなっている。

また、システム企画部は、平成22年10月に日本年金機構システム外部委託実施要領（平成22年要領第60号。以下「システム委託要領」という。）を制定し、機構が行う情報システムの開発、管理、運用及び保守並びにこれらの支援に係る外部委託の実施に際し、契約締結前に必要な仕様書の作成、受託業者の選定及び契約書の作成その他必要な事項について定めている。システム委託要領によると、情報システムの調達等に係る外部委託を実施する場合、事業担当部署は、契約書、調達仕様書及び要件定義書の各案（以下、これらを

合わせて「仕様書案等」という。）を作成し、仕様書等において、受託業者に対して、年金個人情報等を適切に管理するために必要な措置及び情報セキュリティ対策のために必要な措置を講じさせなければならないことなどについて定めることとなっている。そして、事業担当部署は、外部委託を実施する前にシステム企画部に仕様書案等の審査を依頼しなければならないこととなっている（図参照）。

図　情報システムの調達、外部委託等に係る手続（概念図）



⑶　相談・サービス推進部が所管している情報システムの概要等

相談・サービス推進部は、事業担当部署の一つであり、被保険者等からの年金に関する相談に対応する業務をコールセンター等で実施している。同部は、コールセンターにおいて電話による相談に使用するためのコールセンター機器群（以下「CC 機器群」という。）を調達して管理している。CC 機器群は、前記 35 システムの一つであり、構内電話交換機、統計管理装置、ソフトウェア、通話録音装置、操作用パーソナルコンピュータ等により講成されている。

そして、CC 機器群の調達、運用等に要した費用は、令和 2 年 4 月から 5 年 10 月までの間で計 6 億 1871 万余円となっている。

（注 1）　セキュリティ要件　　ポリシーに規定するセキュリティ責任者等が実施する必要がある遵守事項又は基本対策事項

2　検査の結果

（検査の観点、着眼点、対象及び方法）

本院は、合規性等の観点から、情報システムの調達、運用のために実施する保守等業務に係る外部委託は、ポリシー、要件確認要領、システム委託要領等に基づいて適切に実施されているかなどに着眼して、前記の 35 システムを対象として、機構本部において、機器の調達及び保守等業務に係る契約書、仕様書等の関係資料を確認するなどして会計実地検査を行った。

（検査の結果）

検査したところ、前記 35 システムのうち相談・サービス推進部が所管している CC 機器群について、次のような事態が見受けられた。

(1) CC機器群の調達契約等に係るセキュリティ要件の定義又は設定等の状況

CC機器群には通話録音装置が配置され、電話相談を行う被保険者等(以下「相談者」という。)とオペレーターとの間で行われるやり取りは全て同装置に録音される仕組みとなっており、同装置に記録される音声データには基礎年金番号、氏名、生年月日、保険料の納付状況等の年金個人情報が含まれる。したがって、CC機器群については、情報システムとして、年金個人情報等の漏えいなどのリスクを回避するための情報セキュリティ対策を適切かつ確実に実施する必要がある。

しかし、相談・サービス推進部は、CC機器群について、その調達等に当たり、情報セキュリティ対策が必要な情報システムに該当しない事務用の機器等(以下「事務機器」という。)であると判断し、事務機器として取り扱っていた。

このため、同部が2年4月に実施したCC機器群の調達等及び同年9月以降に実施した保守等業務の外部委託に際して、セキュリティ責任者である相談・サービス推進部長は、セキュリティ要件の定義又は設定を行っていなかった。そして、同部は、システム企画部に対する仕様書案等の内容に係る審査の依頼を行っておらず、また、要件確認要領に基づき、2年9月以降は、情報管理対策室に対するセキュリティ要件に係る適合性確認の依頼を行うこととなったのに、2年9月以降に実施する保守等業務の外部委託に際して、これを行っていなかった。

また、システム委託要領によると、外部委託の実施に当たり、仕様書等を作成する場合には、受託業者においてポリシーに適合した情報セキュリティ対策を確実に実施することなどの年金個人情報を保護する上で重要なセキュリティ要件や、受託業者の社員及び再委託先の社員がデータの持ち出しを行わないための対策及び持ち出しを行った場合の対応策等について定めることとなっている。しかし、CC機器群の保守等業務に係る外部委託契約について確認したところ、仕様書等においてこれらの内容が定められていなかった。

(2) CC機器群に係るぜい弱性対策の状況

前記のとおり、CC機器群に配置される通話録音装置には相談者とオペレーターとのやり取りが録音され、その音声データには年金個人情報が含まれる。また、ポリシーによれば、セキュリティ責任者は、ぜい弱性対策を実施するとともに、ぜい弱性対策の状況を定期的に確認し、ぜい弱性対策が執られていない状態が確認された場合等には、ぜい弱性対策計画を策定することなどとされている。

しかし、CC機器群において使用されているOS(オペレーティングシステム)について、製造元からぜい弱性に係る情報が随時公開されるなどしていたにもかかわらず、セキュリティ責任者である相談・サービス推進部長は、これらの情報を把握していなかった。そのため、セキュリティパッチ(注2)を適用するなどのぜい弱性対策を実施しておらず、ぜい弱性対策計画の策定についての検討も行っていなかった。

なお、機構は、3年2月に実施した内部監査により、CC機器群について、ぜい弱性対策が十分でないことなどについて把握していたものの、5年6月に行った機構本部に対する会計実地検査の時点でも、ぜい弱性対策を完了していなかった。

これらのことから、CC機器群については、相談者の年金個人情報を含む録音データが漏えいするなどのリスクが回避されているとは認められない状況となっていた。

（注２） セキュリティパッチ　既に公開されているOSやソフトウェア等において発見されたぜい弱性等に対処するために製造元等から提供されるプログラム

このように、機構において、CC機器群について、ポリシーに基づく適切な情報セキュリティ対策が講じられておらず、相談者の年金個人情報を含む録音データが漏えいするなどのリスクが回避されているとは認められない状況となっていた事態は適切ではなく、改善の必要があると認められた。

（**発生原因**）

このような事態が生じていたのは、情報管理対策室及びシステム企画部において、情報システムの調達、保守等業務に係る外部委託等に当たっては、ポリシー、要件確認要領、システム委託要領等を遵守して行わなければならないことや、情報セキュリティ対策の必要性等の観点から、情報システムと事務機器を適切に分類することについて、事業担当部署に対して十分に周知徹底していなかったこと、相談・サービス推進部において、CC機器群の調達等に当たり、ポリシー等に定められた情報セキュリティ対策の対象となる情報システムとして取り扱う必要があること及び情報システムとしてぜい弱性対策等を適切に実施する必要があることについての認識が欠けていたことなどによると認められた。

3　当局が講じた改善の処置

上記についての本院の指摘に基づき、機構は、次のような処置を講じた。

ア　相談・サービス推進部は、CC機器群について、５年９月末までに、セキュリティ要件の定義又は設定を行い、適合性確認及び仕様書案等の審査を受けるなどした上で保守等業務に係る外部委託契約を締結するとともに、セキュリティパッチの適用等のぜい弱性対策等を実施し、相談者の年金個人情報を含む録音データが漏えいするなどのリスクを回避するための措置を完了した。

イ　情報管理対策室及びシステム企画部は、５年８月に、事業担当部署に対して指示文書を発出して、情報システムの調達、保守等業務に係る外部委託等に当たっては、ポリシー、要件確認要領及びシステム委託要領に基づき、事前に情報管理対策室の確認及びシステム企画部の審査を受ける必要があることや、情報セキュリティ対策の必要性等に関する情報システムと事務機器の分類上の整理及びそれぞれの調達手続について、改めて周知徹底した。