

## 「内閣官房セキュリティ・IT人材確保・育成計画」(概要)

内閣官房の職員は、内閣の重要政策の企画・立案・総合調整のために個々の政策ごとに各府省から出向等により賄われており、一定の任期を経ての所属府省等との異動が頻繁に行われること、所管する情報システムの大半が治安、安全保障等に係る業務に関するもので運用・管理する職員を含めシステムの詳細が明らかにできないことなどから、組織的・体系的に、情報セキュリティ・ITに係る人材確保・育成を行うことが難しいことを踏まえ、一般職員の情報リテラシーの維持・向上を主眼として「内閣官房におけるセキュリティ・IT人材確保・育成計画」を策定する。

内閣官房では、本計画の着実な実施に向けて取り組むものとし、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

### 1. 体制の整備

内閣官房では、内閣総務官室がセキュリティ・ITに係る統括部局を担っているが、内閣官房職員のリテラシー向上に係る研修の拡充、内閣官房が利用する内閣府LANに係る運用業務や、人事給与業務の見直し等業務改革を含む内閣官房内の情報セキュリティ対策の強化や情報化推進の強化を重視し業務遂行体制の強化に必要な機構・定員要求を行う。

### 2. 一般職員の情報リテラシー向上

情報セキュリティに関する一般行政職員のリテラシー向上のため、次の研修を実施する。

- 全職員向け研修（役職別研修も含む）
- 新規異動者向け研修
- 外部研修への積極的参加
- 標的型攻撃メールに対する教育訓練

# 内閣法制局セキュリティ・IT人材確保・育成計画（概要）

平成28年8月31日

内閣法制局

## はじめに

本計画は、内閣法制局が所管する情報システムが主に局内における小規模なシステムに限られることを踏まえ、平成31年度を目途に、当該システムの適切な運用管理及びサイバーセキュリティ対策を図るため、当局の組織規模・人事構成に鑑み、プロパー職員の情報セキュリティ及びITに係る能力の向上に主眼を置き、当局におけるセキュリティ・IT人材確保・育成を図ることを目的として策定するものである。

## 1 体制の整備と人材の拡充

内閣法制局は、小規模な組織であり、また、職員の多くは外部からの出向職員で構成されていることから、情報管理担当部門の体制整備・人材確保には制約がある。このことを踏まえ、同部門に配置されていないプロパー職員においても、情報セキュリティ及びITに係る知識の習得を図ることにより、当局全体の体制を強化・整備することとする。そのため、情報セキュリティ及びITに係る研修の受講等の機会の増大、内閣官房、総務省等との人材交流等について、調整を図ることとする。

### (1) セキュリティ・ITに係る統括部局の体制の整備

サイバーセキュリティ・ITについては、情報管理担当部門のほか、局内各部局に情報セキュリティ管理者を置き、統括情報セキュリティ責任者を通じて、局内全体を統括する体制を構築している。

### (2) 社会的な影響の大きいシステムを所管する部局の体制の整備

内閣法制局においては、社会的な影響の大きいシステムを所管していないことから、その関係の体制の整備を図ることとはしていない。

### (3) 人材の拡充についての方針

プロパー職員は、主たる業務である法令審査事務に関する十分な知識・経験を有する必要があるほか、各種官房事務にも従事させる必要があることから、当該職員全員について、情報セキュリティ及びITに係る能力向上を図ることにより、当局全体の体制を強化・整備することとする。そのため、情報セキュリティ及びITに係る研修の受講等の機会を増大し、内閣官房、総務省等との人材交流等について調整を図ることとするほか、採用に当たっても、それらに係る知識の習得状況等を考慮することとする。

## 2 有為な人材の確保

内閣法制局においては、主たる業務である法令審査事務に配置することを前提とした採用を行っているところ、これに加えて、情報セキュリティ・ITに係る素養、知識の習得状況及び関係業務への意向等も考慮した採用を行うこととする。また、極めて少ないプロパー職員に対し、情報セキュリティ・IT部門に特化したキャリアパスを想定す

ることは困難であるが、研修受講機会の増大を推進するほか、内閣官房、総務省等との人事交流等による人材の登用により、情報管理担当部門に配置されたプロパー職員への技術伝搬（OJT）等を通じて、能力の育成を図っていく。

### 3 セキュリティ・IT人材育成支援プログラム

情報セキュリティ・ITに関する研修については、全職員を対象に総務省において用意する研修等を積極的に受講させるほか、情報管理担当部門に配置する職員には、内閣官房主催の研修への受講、内閣官房等から提供される情報セキュリティ・ITに係る能力向上のための各種情報の積極利用を推進することにより、人材育成を図る。

#### (1) 内閣官房及び総務省において用意する研修の活用

全職員（特にプロパー職員）について、総務省において用意するA、Bレベルの研修を受講させる。また、情報管理担当部門の職員については、同様にレベルDまでの研修の受講を目指すほか、さらに、内閣官房主催の勉強会、研修等への参加を積極的に推進し、情報セキュリティ・ITに係る能力の向上を図る。

#### (2) 出向

現在、総務省との人事交流により、同省情報管理部門の職員の出向を受け入れているところであるが、当局職員の内閣官房、総務省等への出向については、当局の組織規模、人事構成、人材育成の状況等を踏まえ、調整を図っていく。

### 4 人事ルート例（キャリアパスのイメージ）

#### (1) 全体的なキャリアパス像

内閣法制局においては、その組織規模等から、情報管理担当部門に長期間配置することは困難であるが、プロパー職員全員について、情報セキュリティ及びITに係る能力向上を図ることとしており、課長級職員への昇任に際しては、情報セキュリティ・IT知識の習得状況、能力等について十分に勘案する。

#### (2) キャリアパスに含めることが想定される部署と役職

##### ① セキュリティについて経験することが想定される課室と役職

##### ② 情報システム・業務改革について経験することが想定される課室と役職

長官総務室 課長級ポスト

プロパー職員が情報システム及びITに係る知識の習得を図ることにより、当局全体の体制が強化・整備され、職員の全体的な能力等の底上げが図られる。その職員を管理等する立場の課長級ポストへの登用については、一定程度以上の情報システム・業務改革に関する知識等を有することを十分に勘案して行うこととする。

### 5 一般職員の情報リテラシー向上

内閣法制局においては、情報システム及び情報セキュリティに関する一般職員のリテラシー向上のため、次の研修等を行うこととする。

#### (1) 全職員向け研修

- ・研修内容：情報セキュリティ対策
- ・研修対象者：全職員

- ・受講予定者数：毎年８０名程度
- ・実施時期：９月～１０月頃
- ・実施方法：講義形式

## (2) 外部研修への積極的参加

内閣官房が実施する情報セキュリティに係る勉強会等及び総務省が実施する情報システム統一研修等の受講を積極的に推進する。

- ・研修内容：情報セキュリティ、情報システム等
- ・受講対象者：全職員
- ・受講予定者数：研修内容による
- ・実施時期：各研修の実施時期による
- ・実施方法：講義形式、e-ラーニング

## (3) 標的型攻撃メール訓練

- ・研修内容：標的型攻撃メールへの対応
- ・訓練対象者：全職員
- ・実施時期：時期は不定期、複数回実施

## 人事院におけるセキュリティ・IT人材確保・育成計画の概要

平成28年 8月31日

### はじめに

本計画は、人事院で所管する人事・給与関係業務情報システム（以下「人給システム」）や採用試験の受験申込みシステムが多くの個人情報を取り扱うシステムであることを踏まえ、セキュリティ・ITに係る統括部局及び社会的に影響の大きいシステムを所管する部局の体制を整備し、その体制を担う人材としてセキュリティ・ITの専門的知識を有する人材の確保を図ることを目的に策定。

本計画の着実な実施に向けて取り組むものとし、セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、本計画の見直しを行う。

### 体制の整備と人材の拡充

セキュリティ・ITに係る統括部局及び人給システムを管理運用する部局の体制の整備として、サイバーセキュリティ対策の強化と人給システムの安定的運用を重視し、必要な機構・定員要求を行う。また、サイバーセキュリティ対策のための人材拡充及び能力向上に向け、橋渡し人材の候補者については、総務省主催の研修へ参加させるほか、内閣官房内閣サイバーセキュリティセンター（以下「NISC」）等への出向を検討。

### セキュリティ・IT人材育成支援プログラム

情報セキュリティに関する研修については、職員のリテラシー向上を図るため、新規採用職員を対象とした情報セキュリティに係るe-ラーニング研修、管理職員を対象とした情報セキュリティの確保に関する研修会、全職員を対象と

した情報セキュリティに関するe-ラーニング研修を実施。

今後、これらに加え、係員層については、総務省主催の「情報システム入門」の受講を原則とし、セキュリティ・IT統括部局の職員については、同省主催の「情報セキュリティ基礎」、「情報システム入門」及び「電子政府基礎」等についての受講を義務付けるなど資質の向上に努める。

## 人事ルート例（キャリアパスのイメージ）

### （１）全体的なキャリアパス像

情報システムの適切な運用管理とサイバーセキュリティ対策の指揮監督を行う体制を整備し、必要な知識・経験等を有する職員を確保・育成していくことを目指す。情報システムやサイバーセキュリティ対策に関係する経験、知識・能力の習得の観点及びセキュリティ・IT統括部局等の運営等の観点から、採用後のキャリアパスの一例は次のとおり。

#### ◆採用・係員

- ・研修：内閣府主催のExcel技能研修（マクロ/VBAに関すること）又は総務省主催の情報システム統一研修（データ分析技法、情報システム入門）等
- ・所属部署：総務課情報管理室、電子化推進室、人材局試験専門官室等
- ・出向等：NISC、各省行政部門等

#### ◆係長クラス

- ・研修：総務省主催の情報システム統一研修（情報セキュリティ基礎、ネットワーク基礎）等
- ・所属部署：総務課情報管理室情報管理専門官、電子化推進室情報システム専門官、人材局試験専門官、給与第一課情報統計専門官等

- ・ 出向等：NISC、各省行政部門 等

◆課長補佐クラス

- ・ 研修：総務省主催の情報システム統一研修（プロジェクト管理（基礎）、情報システム新任者） 等
- ・ 所属部署：総務課情報管理室情報管理専門官、電子化推進室情報システム専門官、人材局試験専門官、給与第一課情報統計専門官 等
- ・ 出向等：NISC、各省行政部門 等

◆管理職

- ・ 研修：総務省主催の情報システム統一研修（情報セキュリティ管理、プロジェクト管理） 等
- ・ 所属部署：総務課情報管理室長、電子化推進室上席情報システム専門官、人材局次席試験専門官、給与第一課上席情報統計専門官 等
- ・ 出向等：なし

◆サイバーセキュリティ・情報化審議官等

- ・ 研修：総務省主催の情報システム統一研修（情報セキュリティ管理又は技術）、内閣官房主催の情報セキュリティ研修

**（２）キャリアパスに含めることが想定される部署と役職**

情報システムやサイバーセキュリティ対策に係る部署として職員の配置が想定される主な部署・役職等は次のとおり。

**① セキュリティについて経験することが想定される課室と役職**

◆事務総局総務課

- ・ 課長
- ・ 情報管理室長
- ・ 情報管理専門官

- ・ 情報セキュリティ専門官
- ・ 個人情報保護専門官

② 情報システム・業務改革について経験することが想定される課室と役職

◆ 事務総局総務課

- ・ 課長
- ・ 情報管理室長
- ・ 情報管理専門官
- ・ 情報セキュリティ専門官
- ・ 個人情報保護専門官
- ・ 広報室長
- ・ 情報公開専門官

◆ 事務総局参事官付（電子化推進室）

- ・ 参事官
- ・ 上席システム運用専門官
- ・ 上席情報システム専門官
- ・ 上席システム管理専門官
- ・ システム運用専門官
- ・ 情報システム専門官
- ・ システム管理専門官

◆ 人材局試験課

- ・ 課長
- ・ 人材局試験課試験監理専門官
- ・ 試験情報専門官

◆ 給与局給与第一課

- ・ 上席情報統計専門官
- ・ 情報統計専門官



③ 事案対処、保安、事故対応、危機管理、安全保障等について経験するこ  
とが想定される課室と役職

◆事務総局総務課

- ・ 課長
- ・ 情報管理室長
- ・ 情報管理専門官
- ・ 情報セキュリティ専門官
- ・ 個人情報保護専門官

④ 一般行政事務について、特に経験をさせたい部署の業務及び想定される  
課室

◆事務総局（院内の調整業務等）

- ・ 総務課
- ・ 企画法制課
- ・ 人事課

**一般職員の情報リテラシー向上**

今後の一般職員の情報リテラシーの向上に向け、現在行っている情報セキュ  
リティに係るe-ラーニング研修等に加え、総務省等の主催研修を積極的に受講  
させる。

◆全職員向け研修

- ・ 研修内容：情報セキュリティ研修
- ・ 受講対象者：全職員
- ・ 受講予定者：毎年600名程度
- ・ 実施時期：10月から12月の間の一定期間
- ・ 実施方法：e-ラーニング

◆新規採用職員向け研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：新規採用職員
- ・受講予定者：毎年10数名程度
- ・実施時期：毎年4月
- ・実施方法：講義形式

◆新規異動者向け研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：新規採用職員等
- ・受講予定者数：年間160名程度
- ・実施時期：職員となった日から3か月以内に適宜実施
- ・実施方法：e-ラーニング

◆管理職員向け研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：新たに管理職員となった者
- ・受講予定者数：年度により異なる（本年度は30名程度）
- ・実施時期：4月又は5月
- ・実施方法：幹部職員による講義形式

**施行期日等**

本計画は、制定の日から施行し、平成33年4月1日までの間において実施。

以 上

## 内閣府本府セキュリティ・IT 人材育成計画(概要版)

内閣府本府が所管する情報システムは、内閣府LANが、内閣府本府のみならず、内閣官房、復興庁、個人情報保護委員会においても使用される共通基盤システムであり、その機能の維持に加え、一段と高い情報セキュリティが求められる。また、個人情報等の機微な情報を取り扱う個別業務情報システムを含む内閣府本府の各部局が運用管理する個別業務情報システムについて、情報システムの適切な運用管理、サイバーセキュリティ対策等を確保する必要がある。

しかしながら、平成 27 年 5 月には日本年金機構によるサイバー攻撃に伴う情報流出事案が発生する等、サイバーセキュリティに対する脅威は増大する中で、①セキュリティに係る人材が圧倒的に不足していること、②システム管理や業務改革に関する知識・経験を有する人材も不足していること、③一般職員の情報リテラシーも不十分であること、④内閣府本府におけるセキュリティ対策等の司令塔機能も弱体であること、⑤組織の新設・改編が頻繁に起こり、人の入れ替わりが多いこと等を踏まえ、平成 28 年度から平成 31 年度の 4 年間を対象として、「内閣府本府セキュリティ・IT 人材確保・育成計画」を策定。

### 1 体制の整備と人材の拡充

セキュリティ・ITに係る情報化参事官が統括する部局の体制の整備として、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれと一体となった業務改革等を重視し必要な機構・機構要求を行う。また、人材の拡充及び能力の向上のために、内閣サイバーセキュリティセンター(NISC)への職員の出向、新人等に対するセキュリティ・ITに関する各種研修に関する研修の実施等を行う。

#### (1)セキュリティ・ITに係る統括部局の体制の整備

サイバーセキュリティ・情報化参事官を専任のサイバーセキュリティ・情報化審議官に格上げし、平成 29 年度における機構要求を実施。

#### (2)人材の拡充についての方針

今後、以下に示す一定の方針の下に人材を拡充させていく。

- ① 内閣府本府内の大臣官房各課やサイバーセキュリティ・情報化推進室及び個別業務情報システムを有する部門を経験し、府内のシステム、サイバーセキュリティ、サイバー上の課題に対する理解を深めさせる。
- ② NISC 等情報セキュリティ関係府省への出向により、サイバーセキュリティ等に関する業務を経験させる。
- ③ 通常、2年での人事異動を、情報セキュリティ担当者に関しては、2年以上

の配置とすることを検討する。

## 2 有為な人材の確保

毎年度、適性が認められる者を候補として、育成していくことを視野に入れた一般職の新卒採用を2～3年に1回1名程度を採用することを検討。また、採用時の面接等においては、情報セキュリティやITに係る素養（専攻分野、資格の取得状況など）を確認し、適性のある人材の確保に努める。

「橋渡し人材」については、プロパー職員の育成を基本とするが、当面は専門的知見を有する民間経験者の採用を行うこととする。現在の取組みとしては、平成24年度から5年間の任期で、民間から1名の採用を行っているが、今後も同様の採用を行うことを検討。

## 3 セキュリティ・IT人材育成支援プログラム

役職段階ごとの研修受講、NISC・情報通信技術（IT）総合戦略室・総務省行政管理局・個人情報保護委員会への出向、国内外の大学院・民間企業への派遣、情報通信研究機構（NICT）が整備する人材育成施設の活用などを通じ、一定の専門性を有する人材を育成することを検討する。

### (1)研修

内閣官房・総務省が実施する「橋渡し人材」向けの研修について、平成29年度に想定される受講者数は延70名程度を見込む。

### (2)出向等

「橋渡し人材」のNISCへの出向について、平成29年度に想定される役職段階別の出向者数は、1名程度を見込む。

## 4 キャリアパス

### (1) 全体的なキャリアパス像

一般職について、採用後に想定されるキャリアパスの一例は以下のとおり。

#### ○ 採用・係員

- ・ 研修：内閣官房及び総務省が提供するレベルA、B研修
- ・ 所属部局：サイバーセキュリティ・情報化参事官が統括する部局（サイバーセキュリティ・情報化推進室）のほか、予算・調達担当部局又は個別業務情報システム運用の各部局を配置先に含める。
- ・ 出向等：NISC等

- 係長クラス（一般職で概ね8年目以降・・・異動状況により変動）
  - ・研修：内閣官房及び総務省が提供するレベルC，D研修
  - ・所属部局：サイバーセキュリティ・情報化参事官が統括する部局（サイバーセキュリティ・情報化推進室）のほか，予算・調達担当部局又は個別業務情報システム運用の各部局を配置先を含める。
  - ・出向等：NISC等
  
- 補佐クラス（一般職で概ね20年目以降・・・異動状況により変動）
  - ・研修：内閣官房及び総務省が提供するレベルC，D研修
  - ・所属部局：サイバーセキュリティ・情報化参事官が統括する部局（サイバーセキュリティ・情報化推進室）のほか，予算・調達担当部局又は個別業務情報システム運用の各部局を配置先を含める。
  
- 管理職（一般職で相当数年後の選考による）
  - ・研修：内閣官房及び総務省が提供するレベルD研修
  - ・所属部局：サイバーセキュリティ・情報化参事官が統括する部局（サイバーセキュリティ・情報化推進室）

## (2) キャリアパスに含めることが想定される部署と役職

### ①サイバーセキュリティについて経験することが想定される課室と役職

- i) サイバーセキュリティ・情報化推進室
  - ・副室長
  - ・室長補佐(情報セキュリティ係)
  - ・係長(情報セキュリティ係)

### ②情報システム・業務改革について経験することが想定される課室と役職

- i) サイバーセキュリティ・情報化推進室
  - ・副室長
  - ・室長補佐(情報システム係)
  - ・係長(情報システム係)
  
- ii) 個別業務情報システムのPJMO、運用担当の課室

## 5 一般職員のリテラシー向上

新人研修等においてセキュリティに関する各種研修を実施、さらに、職員に

対してeラーニング等による実施や、そのためのセキュリティ・IT教材の最新化なども併せて検討。講習、訓練、講演などについては、延7200名程度/年を見込む。特に、組織の新設・改編が頻繁に起こり、人の入れ替わりが多いことから、役職別等にかかわらず、主要な講習については、通年で受講ができる体制を整えている。

以上

## 宮内庁セキュリティ・IT人材確保・育成計画（概要版）

### はじめに

近年の政府機関等を対象としたサイバー攻撃事案の増加等に鑑み、宮内庁においても、情報システムの運用管理と情報セキュリティ対策及びこれらと一体となった業務改革等に取り組み、セキュリティを確保しつつ効率的な行政運営の実現を図ることが必要である。

情報システムの適切な運用管理と情報セキュリティ対策の指揮監督を行う組織については、宮内庁の情報システム数の規模（6つ）も考慮しつつ、引き続き、その強化を図る。そして、限られた体制の中でも最大限の対応ができるよう、有為な人材の確保に努め、達成すべき専門知識・能力のレベルを明確にした上で、それらを習得させるべく、適切に育成を行う。

以上を目的として、平成28年度から平成31年度の4年間を対象に、以下のとおり「宮内庁におけるセキュリティ・IT人材確保・育成計画」を策定する。

なお、本計画は、必要に応じて、適切かつ柔軟に見直しを行っていくこととする。

### 1. 体制の整備と人材の拡充

#### 宮内庁のセキュリティ・ITに係る専任体制

平成9年度 長官官房秘書課調査企画室に情報係長を設置

平成11年度 情報係員を設置

平成19年度 情報セキュリティ対策専門官（調査企画室長補佐と兼務）を設置

平成28年度 情報技術専門官を設置（民間から登用）

今後は、本計画に基づき、更なる体制の整備を進めていく。

また、人材の拡充及び能力の向上のために、セキュリティやITに係る素養のある人材の新卒採用、専門的知見を有する民間経験者の採用、セキュリティ・ITの統括部局及び関連部局への配置、内閣官房及び総務省の研修の活用等を実施する。

### 2. セキュリティ・IT人材育成支援プログラム

#### 橋渡し人材及びその候補者を対象

- ・内閣官房及び総務省が提供する研修の積極的な活用
- ・橋渡し人材の育成のためには、インシデントレスポンスに関する業務経験や情報システム改革に関する業務経験は有意義であると考えられるため、これらの業務を所掌する政府部内機関への出向について検討する。
- ・CSIRT構成員については、上記育成のほか、宮内庁に対するサイバー攻撃への対処に特化した初動対応教育・訓練を行う。CSIRT構成員以外の職員であっても、CISOが相応しいと認めた者については、その参加を認める。

### 3. 人事ルート例

#### (1) 全体的なキャリアパス像

橋渡し人材及びその候補者については、情報セキュリティ・ITの統括部局を軸に、予算・調達担当部局、情報システム運用部局等の関連部局を経験させることによって、実践的な知見や応用力を身に付けさせ、将来的には、適性に応じて管理職ポストへの配置も行う。

#### (2) キャリアパスに含めることが想定される部署と役職

##### ① セキュリティについて経験することが想定される課室と役職

###### i) 長官官房秘書課調査企画室

・室長，室長補佐（情報係担当），情報技術専門官，情報係長

##### ② 情報システム・業務改革について経験することが想定される課室と役職

###### i) 宮内庁情報ネットワークシステム所管

長官官房秘書課調査企画室

・室長，室長補佐（情報係担当），情報技術専門官，情報係長

###### ii) 宮内庁公開システム所管

長官官房総務課報道室

・室長，室長補佐（広報係担当），広報専門官，広報係長

### 4. 一般職員の情報リテラシー向上

一般職員の情報システム及び情報セキュリティに関するリテラシー向上のため、次の研修等を行う。

- ・新規採用職員向け研修（講義形式）
- ・情報セキュリティ責任者及び同副責任者向け研修（個別及び小講義形式）
- ・全職員向け研修（講義形式に加え、研修資料を全庁掲示板に掲載して周知）
- ・全職員向け標的型メール攻撃訓練（毎年度実施、時期は不定期）



# 公正取引委員会セキュリティ・IT人材確保・育成計画（概要版）

平成 28 年 8 月 31 日  
最高情報セキュリティ責任者／情報化統括責任者  
官房総括審議官

## はじめに

### （1）経緯

公正取引委員会においては、近年、情報セキュリティ及び情報システムに関する知識を習得させるため、情報システム担当部署に所属する職員を中心として、一般職員及び管理職を対象とした研修等を実施することによりセキュリティ・IT人材を育成してきた。

他方、サイバーセキュリティ対策推進会議（CISO等連絡会議）・各府省情報化統括責任者（CIO）連絡会議において「政府機関におけるセキュリティ・IT人材育成総合強化方針」（平成 28 年 3 月 29 日）が決定され、同方針において、各府省庁の統括部局の体制の整備及び人材の拡充を行い、併せて各府省庁の一定のシステム所管部署の体制の整備及び人材の拡充を行うことが求められていることから、公正取引委員会においても、現状以上にセキュリティ・IT人材の確保・育成を行う必要がある。

### （2）目的

本計画は、公正取引委員会で所管する情報システムにおいて、セキュリティに関する人材が必要であると共に、システム管理や業務改革に関する知識・経験を有する人材が必要であることを踏まえ、平成 31 年度を目途に、情報システムの適切な運用管理とサイバーセキュリティ対策の指揮監督をする組織として、司令塔機能を有する体制を充実し、その体制を担う人材として橋渡し人材等の確保を図ることを目的に、以下のとおり「公正取引委員会におけるセキュリティ・IT人材確保・育成計画」として策定したものである。

公正取引委員会では、本計画の着実な実施に向けて取り組むものとし、セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

## 1. 体制の整備と人材の拡充

公正取引委員会では、平成 28 年度からサイバーセキュリティ・情報化参事官の新設により、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等について、強力な体制を構築することとしている。このため、平成 29 年度において、サイバーセキュリティ・情報化参事官の下の体制（以下「情報システム室」という。）の強化に必要な機構・定員の要求を行う。

また、情報システム室及び審査局システム担当部署における人材の拡充並びに当該職員の能力の向上のために今後 4 年間に於いて、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）等への職員の出向、職員に対するセキュリティ・

ITに関する研修の実施等を行う。

## **2. 有為な人材の確保**

一般職として新規採用した職員の中から、2年間に1名程度橋渡し人材候補として育成していくことを視野に入れた採用活動を行う。その際、採用時の面接等で情報セキュリティやITに係る素養及び関係業務への意向を確認することとする。新卒採用により確保した人材については、OJT、出向、研修等を通じてセキュリティ・IT関係の業務処理に関する能力等の育成、適正性の有無の判断等を行うものとする。

また、橋渡し人材については、最終的には新卒採用者からの育成を基本としつつ、当面はセキュリティ・IT関係の人材の確保が必要であることから、官民人事交流の枠組みを使った採用や、民間企業等におけるセキュリティ・IT関係業務に携わった経験のある者を必要に応じて中途採用していく。なお、採用に当たっては、公正取引委員会における一般行政事務への志望のみならず、セキュリティ・IT関係業務への意向及びこれまでに経験した業務内容や資格等を確認することとする。中途採用により確保した人材については、OJT、出向、研修等を通じてセキュリティ・IT関係の業務処理に関する能力の育成に加え、研修やOJTを通じた一般行政事務についての育成も併せて行うものとする。

## **3. セキュリティ・IT人材育成支援プログラム**

公正取引委員会では、橋渡し人材が受講すべき研修については、総務省行政管理局が実施する情報システム統一研修及び内閣官房が実施する研修等を活用し、毎年数名程度の受講を目途にそれぞれ実施していくものとする。また、出向等については、当面は、セキュリティ関係としてのNISC、又はIT関係としての内閣官房情報通信技術（IT）総合戦略室（以下「IT総合戦略室」という。）のいずれかに、2年間で1名程度を派遣することを目途に関係機関との調整等を行うものとする。

また、研修によって得られた成果を人事評価等により、セキュリティ・ITに関する能力やスキルの観点から適切に評価していく。

## **4. 人事ルート例（キャリアパスのイメージ）**

### (1) 全体的なキャリアパス像

公正取引委員会では、情報システムの適切な運用管理とサイバーセキュリティ対策を指揮監督する体制を整備し、必要な知識、経験を有する職員を確保・育成していくこととしている。こうした情報システムやサイバーセキュリティ対策に係る経験や知識・能力の習得の観点から、公正取引委員会採用後に想定されるキャリアパスの一例は次のとおりである。

◆採用・係員（採用年から6年目頃まで）

情報セキュリティ及びITに関する基礎的な知識・技能に関する研修を受講させる。

所属部署については、情報システム室又は審査局システム担当部署を一度以上経験させる。

◆係長クラス（6年目頃から18年目頃まで）

情報セキュリティ及びITに関する上位者から要求された作業が可能となる応用的知識・技能に関する研修を受講させる。

所属部署については、情報システム室又は審査局システム担当部署を一度以上経験させる。

また、NISC又はIT総合戦略室への出向や、セキュリティ・IT系の大学院への派遣を経験させる。

◆課長補佐クラス（18年目頃以降）

情報セキュリティ及びITに関する独力で高度な作業を行うことができる専門的知識・技能に関する研修を受講させる。

所属部署については、情報システム室又は審査局システム担当部署を一度以上経験させる。

◆管理職

情報セキュリティ及びITに関するプロジェクト管理と下位者への指導・育成が可能となる高度な専門的知識・技能に関する研修を受講させる。

サイバーセキュリティ・情報化参事官以外の管理職を経験させる。

◆サイバーセキュリティ・情報化参事官

情報セキュリティ及びITに関するプロジェクト創造と下位者への指導・育成が可能となる高度な専門的知識・技能に関することを受講させる。

(2) キャリアパスに含めることが想定される部署と役職

公正取引委員会において、情報システムやサイバーセキュリティ対策に関係する部署として職員の配属が想定される部署・役職等は次のとおりである。

① セキュリティについて経験することが想定される課室と役職

i) 情報システム室

- ・官房サイバーセキュリティ・情報化参事官
- ・課長補佐
- ・係長
- ・係員

ii) 審査局システム担当部署

- ・審査局企画室長
- ・課長補佐

- ・係長
- ・係員

② 情報システム・業務改革について経験することが想定される課室と役職

i) 情報システム室

- ・官房サイバーセキュリティ・情報化参事官
- ・課長補佐
- ・係長
- ・係員

ii) 審査局システム担当部署

- ・審査局企画室長
- ・課長補佐
- ・係長
- ・係員

③ 一般行政事務について、特に経験をさせたい部署の業務及び想定される課室と役職

独占禁止法等の違反事件審査関係業務，企業結合の審査業務

## 5. 一般職員の情報リテラシー向上

公正取引委員会では、情報システム及びセキュリティに関する一般行政職員のリテラシー向上のため、次の研修を実施することとしている。

### ○全職員向け研修

i) 情報セキュリティ強化週間 eラーニング研修

- ・研修内容：セキュリティ・個人情報保護について
- ・受講対象者：全職員
- ・受講予定者数：毎年 900 名程度
- ・実施時期：第 2 四半期
- ・実施方法：eラーニング

ii) 一般職員向け eラーニング研修

- ・研修内容：セキュリティについて
- ・受講対象者：全職員
- ・受講予定者数：毎年 900 名程度
- ・実施時期：第 4 四半期
- ・実施方法：eラーニング

### ○階層別研修

以下に記載の階層別研修のほか、必要に応じ行っていく予定。

i) 新規採用者向け研修

- ・研修内容：セキュリティ・ITについて

- ・受講対象者：新規採用者
  - ・受講予定者数：毎年 30 名程度
  - ・実施時期：毎年 4 月（セキュリティ約 1 時間、情報システム約 3 時間のコース）
  - ・実施方法：情報セキュリティ・IT 担当者からの講義形式
- ii) 総括業務新任者研修（係長級）
- ・研修内容：セキュリティ・IT について
  - ・受講対象者：総括業務に従事する係長相当職
  - ・受講予定者数：毎年 15 名程度
  - ・実施時期：7 月（30 分のコース）
  - ・実施方法：情報セキュリティ・IT 担当者からの講義形式
- iii) 新任管理職向け講習（管理職級）
- ・研修内容：セキュリティ・IT について
  - ・受講対象者：一般行政事務に従事する管理職昇任 1 年以内の職員
  - ・受講予定者数：毎年数名
  - ・実施時期：7 月又は 8 月（1 時間のコース）
  - ・実施方法：官房サイバーセキュリティ・情報化参事官からの講義形式
- iv) 管理職向け研修（管理職級）
- ・研修内容：セキュリティについて
  - ・受講対象者：一般行政事務に従事する管理職相当職
  - ・受講予定者数：毎年 100 名程度
  - ・実施時期：毎年 2 月（1 時間のコース）
  - ・実施方法：CISO アドバイザー兼CIO 補佐官による講義形式

以上

# 警察庁サイバー人材確保・育成計画

- 政府にあっては、情報システムとセキュリティ対策に係る体制強化を図るため、各府省庁においてセキュリティ・IT人材（橋渡し人材）に係る採用、人材育成、将来像等にわたる具体的な取組方策を策定することを決定
- 警察においては、次の人材の育成が必要
  - ◆ 橋渡し人材
  - ◆ 情報通信部門において情報通信技術関連の業務に従事する高度専門人材
  - ◆ サイバー空間の脅威への対処に従事する警察官

## サイバー人材の確保

橋渡し人材



高度専門人材



サイバー空間の脅威への対処に従事する警察官



警察情報通信学校等



学校  
研修等

情報通信部門



互いの能力・  
知見を活用

サイバーセキュリティ  
対策研究・研修センター等

サイバーセキュリティ対策

サイバーセキュリティ運営

サイバー犯罪捜査指揮

サイバー攻撃捜査指揮

サイバー犯罪(応用)

サイバー攻撃(応用)

サイバー犯罪・攻撃(基礎)

サイバー  
犯罪対策

サイバー  
攻撃対策

研修



技術系職員採用

# 警察庁サイバー人材確保・育成計画

## 基本的考え方

サイバー空間が国民生活や経済活動に不可欠な社会基盤として定着し、サイバー空間と実空間がますます融合する中、サイバー空間があらゆる犯罪に悪用され得るようになっており、今やサイバー空間の安全なくして治安は成り立たない。そのため、サイバー空間の脅威への対処機関としての警察の質的・量的な能力向上は、部門を問わず喫緊の課題となっている。同時に、効率的な警察運営の実現のためには、情報通信技術の利活用を通じ、第一線の捜査活動等様々な警察活動を支援することが不可欠であるとともに、警察が国民の信頼を得るためには、自らのサイバーセキュリティの確保が大前提であることから、警察にあってはその両立を図らなければならない。

警察庁では、警察通信、情報の管理、犯罪の取締りのための情報技術の解析等を担わせるため、従前から警察官とは別に総合職及び一般職の技術系職員を採用し、情報通信部門を中心に配置して運用してきた。また、平成28年4月には長官官房にサイバーセキュリティ・情報化審議官を、情報通信局情報管理課に情報セキュリティ対策官を新設し、警察庁及び都道府県警察並びに所管法人における業務について、サイバーセキュリティの確保、情報システムの整備及び管理並びにこれらと併せて行われる事務の運営の改善及び効率化を図るための体制を強化するなど、内部部局における体制整備に努めるとともに、警察大学校附属警察情報通信学校における教育訓練を通じて、警察が必要とする能力や高度な専門的・技術的能力を有する人材の育成・充実も図ってきた。加えて、警察がサイバー空間の脅威に関する的確な捜査活動を行うため、警察大学校サイバーセキュリティ対策研究・研修センターを頂点とした研修体系等の人材育成基盤を充実してきたところである。

今後は、情報通信技術が日進月歩で進展する時代の要請に応え続けるため、警察運営全体の企画から実施に至る様々な段階において、情報通信に係る知識・技術を駆使できるよう、これらの態勢の持続的強化を図るとともに、警察官と技術系職員とが互いの能力・知見を更に活用できる方策を実現し、警察の人的基盤を強化するほか、全警察職員の情報システムに関するリテラシー等の向上にも取り組む必要がある。

本計画は、上記のとおり我が国のサイバーセキュリティにおいて警察が占める位置付け及び政策課題を踏まえ、2020年東京オリンピック・パラリンピック競技大会等の大規模な国際行事の開催を見据え、サイバー空間も含めた治安の維持に万全を期すとともに、警察運営の更なる効率化を推進するため、警察庁におけるサイバー人材として、情報通信部門における高度な専門的知識・技能を有する人材（以下「高度専門人材」という。）及び情報通信技術に関する一定の専門性と所管行政に関する十分な知識、技能、経験を有し、高度専門人材と一般行政部門との橋渡しをする人材（以下「橋渡し人材」という。）並びにサイバー空間の脅威への対処に係る警察官の確保・育成を図ることを目的に、「警察庁サイバー人材確保・育成計画」として策定したものである。

警察庁では、本計画の着実な実施に向けて取り組むものとし、サイバー人材の確保・育成状況等を踏まえ、必要に応じて、適切かつ柔軟に本計画の見直しを行っていく。

## 第1 体制の整備

警察庁では、サイバー空間の脅威への対処、情報通信技術の利活用による効率的な警察運営の実現及び自らのサイバーセキュリティの確保の両立を担う体制整備に努めているところ、昨今のサイバーセキュリティ情勢の深刻化等を踏まえた機構・定員要求を行う。

## 第2 人材の拡充

警察庁では、一般職及び総合職の技術系職員について、新卒採用に当たり、橋渡し人材・高度専門人材の候補として位置付けた採用活動を行うとともに、採用後は、情報通信部門を中心とする関係部局への配置、部内外における研修、OJT等を通じて情報通信技術に係る知識・技能向上を図りつつ、適性に応じて計画的に育成していく。

また、都道府県警察では、サイバー空間の脅威への対処に従事する警察官の育成について、「警察におけるサイバーセキュリティ戦略」（平成27年9月4日付け警察庁乙官発第13号ほか別添）を受けて策定した「サイバー空間の脅威への対処に係る人材育成方針」（平成27年12月22日付け警察庁丙総発第85号ほか別添。以下「警察人材育成方針」という。）に基づき、能力を有する者の積極的な採用・登用や職員の更なる能力向上を図る。

### 1 有為な人材の確保

#### (1) 一般職及び総合職の技術系職員

##### ア 橋渡し人材・高度専門人材の候補の採用

警察庁情報通信部門では、毎年度、一般職及び総合職の技術系職員を新卒採用により確保（平成29年度は100名程度を予定）している。特に一般職の採用活動では、管区警察局、北海道警察情報通信部及び東京都警察情報通信部（以下「地方機関」という。）において現場業務を担っている実情を踏まえ、既に確立している多様なキャリアパスを示し、応募者の勤務地や待遇に関する多様な志望に応えることで、質的・量的な水準を維持している。今後、採用時面接等において、情報通信技術に係る素養を確認するとともに、橋渡し人材・高度専門人材としての業務内容を一層丁寧に説明する。

また、情報通信技術に係る実践的な知識・技能を有する人材を確保するため、大学の学生を対象としたものに加え、高等専門学校の子生を対象とした業務説明会等を積極的に実施する。

さらに、従来から一般職国家公務員待遇として、一般職試験による採用のほか、第一級陸上無線技術士資格保有者からも採用しているところ、今後は、新たに創設された情報処理安全確保支援士資格等関連する資格の保有者からの採用等についても検討する。

加えて、高度専門人材の候補を見据え、採用の段階から突出した能力を有する人材を発掘することも重要である。現在、若年層における人材の裾野を拡大し、世界に通用するトップクラス人材を創出するため、官民を挙げて、グローバル水準の能力を競うコンテストや研究成果を発表する国際会議等が開催されており、警察庁も参画してきた。これらは、突出した能力を持ちうる人材を発掘することができる“場”としても機能することから、今後は、警察の有する高度な専門性や魅力的なキャリア形成等について情報発信するなど、一層の人材発掘に努める。



## イ 適切な処遇

警察庁では、所管する情報システムの開発・構築、サイバーセキュリティの確保、所管行政における情報化の推進、犯罪の取締りのための情報技術の解析、その他警察に係る情報通信に関する研究に関する業務分野のうち、特に高度な専門的知識・技能を要する業務については、高度専門人材を配置し担当させている。

高度専門人材は、情報通信部門の技術系職員について、地方機関における業務実績や警察大学校等における研修の成績等を通じ、特に適性の高い者を発掘するとともに、本人の志望等を尊重した上で年功序列に捕らわれず、長期特別研究制度等を通じて警察庁における高度な実務に従事させるなど、内部部局、附属機関及び地方機関ごとの特性を踏まえたキャリアパス管理を実施しながら、より高いレベルの研修や該当部署でのOJT等を通じて育成している。今後は、最新の技術に対応した研修の充実等により人材の拡充を図る。特に、「サイバーセキュリティ人材育成総合強化方針」（平成28年3月31日サイバーセキュリティ戦略本部決定。）第2章の2（5）に基づき、セキュリティ・ITに係る業務の専門性・特殊性等を踏まえ、政府において手当等を新たに支給することによる一定の給与上の評価を行うこととされたことから、既に一定の人材を確保している警察庁においては、政府の取組を活用し、業務実績や保有資格に応じた諸手当の充実等処遇の改善を検討する。

また、高度専門人材のうち、全国的にみて極めて卓越した情報通信に関する能力を有する人材については、上席技術者に指定し、本人の意向を踏まえた人事配置に配慮し、高度な実務、研究開発、外部機関との交流による技術情報の共有・収集、後進の指導等を集中的に行わせるなど、その能力を最大限発揮させるような運用に努めている。指定された者は、称号及びその者の有する情報通信に関する能力を表す別号が付与され、全ての技術系警察情報通信職員の目標となっており、今後とも、こうした取り組みを通じて、技術系職員全体の士気高揚を図る。

### (2) サイバー空間の脅威への対処に従事する警察官

サイバー犯罪やサイバー攻撃といったサイバー空間の脅威への対処に従事する警察官については、素養ある優秀な人材を確保するため、警察人材育成方針に基づき、都道府県警察における計画的な採用、積極的な採用募集活動及び民間事業者からの採用・登用を推進する。

## 2 人材の育成

### (1) 研修

#### ア 一般職及び総合職の技術系職員

##### ○ 学校研修

警察庁では、警察業務の特殊性を踏まえ、警察大学校附属警察情報通信学校において、一般職又は総合職として採用された全ての技術系職員に対し、情報通信部門の業務に必要となる基本的な知識・技能を習得させるための研修や情報通信技術に係る特定の業務分野における高度な専門的知識・技能を習得させるための研修を実施している。今後は、講義内容の充実や短期コースの新設による入校機会の増加等を図る。

## ○ 外部委託研修等

警察庁では、一般に普及していない最新の技術に関する知識・技能等、研修環境を警察庁で用意することが困難な場合についても、必要に応じ民間企業が提供する研修や国内外の大学等学術機関に対する派遣等を通じて習得に努めており、引き続き活用を図る。

## ○ 内閣官房及び総務省において用意する研修

警察庁では、一般的なITスキルや電子政府に関するものなど、政府機関に共通する知識・技能に関する研修については、内閣官房及び総務省において用意する研修を活用している。今後は、現に統括部局や社会的な影響の大きいシステムを所管する部局で勤務している職員については、本研修を積極的に活用するとともに、それら以外の職員についても、積極的な受講を推奨する。

## ○ その他

警察庁では、警察庁CSIRTの対処能力向上を図ることを目的とした実践的訓練を毎年実施している。

## イ サイバー空間の脅威への対処に従事する警察官

サイバー空間の脅威への対処に従事する警察官については、警察人材育成方針に基づき、警察大学校サイバーセキュリティ対策研究・研修センター、警察庁内部部局、管区警察局及び都道府県警察における研修を活用するほか、情報通信技術に係る高度な専門性を有している民間事業者、大学等の学術機関等による講義・研修や民間事業者等への派遣を図ることにより、人材を育成する。

また、人材の裾野の拡大等のため、警察庁において、平成29年度以降、研修体系の見直しを図る。

## (2) 配置

### ア 一般職及び総合職の技術系職員

#### ○ 部内配置

実践的な知識・技能を習得する上では、OJTは不可欠である。特に、知識・技能の陳腐化を避けるため、実務に従事することは重要である。その際、橋渡し人材については、情報通信部門の経験に加えて、情報システムが運用される業務の主管部門の経験を必要とする一方、高度専門人材については、高度な実務に没頭できる環境を必要とするなど、職員個人の将来の人材像に留意して配置しなければならない。

そのため、警察庁では、総合職及び一般職の技術系職員について、採用後のキャリアアップの過程において別紙のとおり、全国の情報通信部門を中心に、都道府県警察、他省庁等の関連部署への組織・部門横断的な人事配置を実施し、技術担当としての様々な経験を積ませることで、情報システムの開発・構築やサイバーセキュリティの確保に関係する知識・技能を組織的に習得させている。引き続き、本人の年次、適性、勤務希望、関係部署からの要望等を踏まえて配置するポストを総合的に判断するとともに、OJT、自己研鑽を支援するツールの導入についても検討していく。

## ○ 人事交流

現在、警察庁では、橋渡し人材及び高度専門人材について、内閣官房内閣サイバーセキュリティセンターや内閣官房情報通信技術（IT）総合戦略室に対し、職員を出向等させている。

こうした場において、セキュリティ・ITに関わる職員が府省庁の垣根を越えて触れ合うことは、職員個人の人的関係や視野の広がり等において有益な効果を見込めることから、引き続きこれら機関との人事交流についても活用を図る。

## イ サイバー空間の脅威への対処に従事する警察官

サイバー空間の脅威への対処に従事する警察官については、警察人材育成方針に基づき、都道府県警察において、職員のサイバー関連部署への勤務希望、情報通信技術に関する知識・技能、保有資格等を組織的に把握するとともに、人材の育成に配意して部門横断的に人材を配置するなど、キャリアパス管理を推進する。

## 3 全警察職員のサイバーリテラシーの向上

警察庁及び都道府県警察では、全警察職員の情報セキュリティ及び情報システムに関するリテラシー向上のため、警察大学校、管区警察学校、都道府県警察学校等において、採用時、昇任時、各部門任用時等に情報セキュリティ対策に関する研修を実施する。

また、平成5年度から継続して実施している警察職員の情報処理能力についての検定により、警察における情報セキュリティポリシーを始めとした情報処理に係る法令・規程に関する知識や情報システムの操作に関する知識・技能を検定し、全警察職員のリテラシー向上を図るほか、上級の区分においてシステムの設計・開発・監査等に係る知識・技能を検定し、情報通信技術に係る人材の拡大を図る。

さらに、国民からの要望、相談等の警察業務において、サイバー空間の脅威についての適切な理解に基づいて対応することが求められていることから、警察庁及び都道府県警察において、警察人材育成方針に基づき、全警察職員を対象としたサイバー空間の脅威の情勢等に関する講演や採用・昇任時研修を実施するなどにより、全警察職員のサイバー空間の脅威への対処に係る知識の底上げを図る。

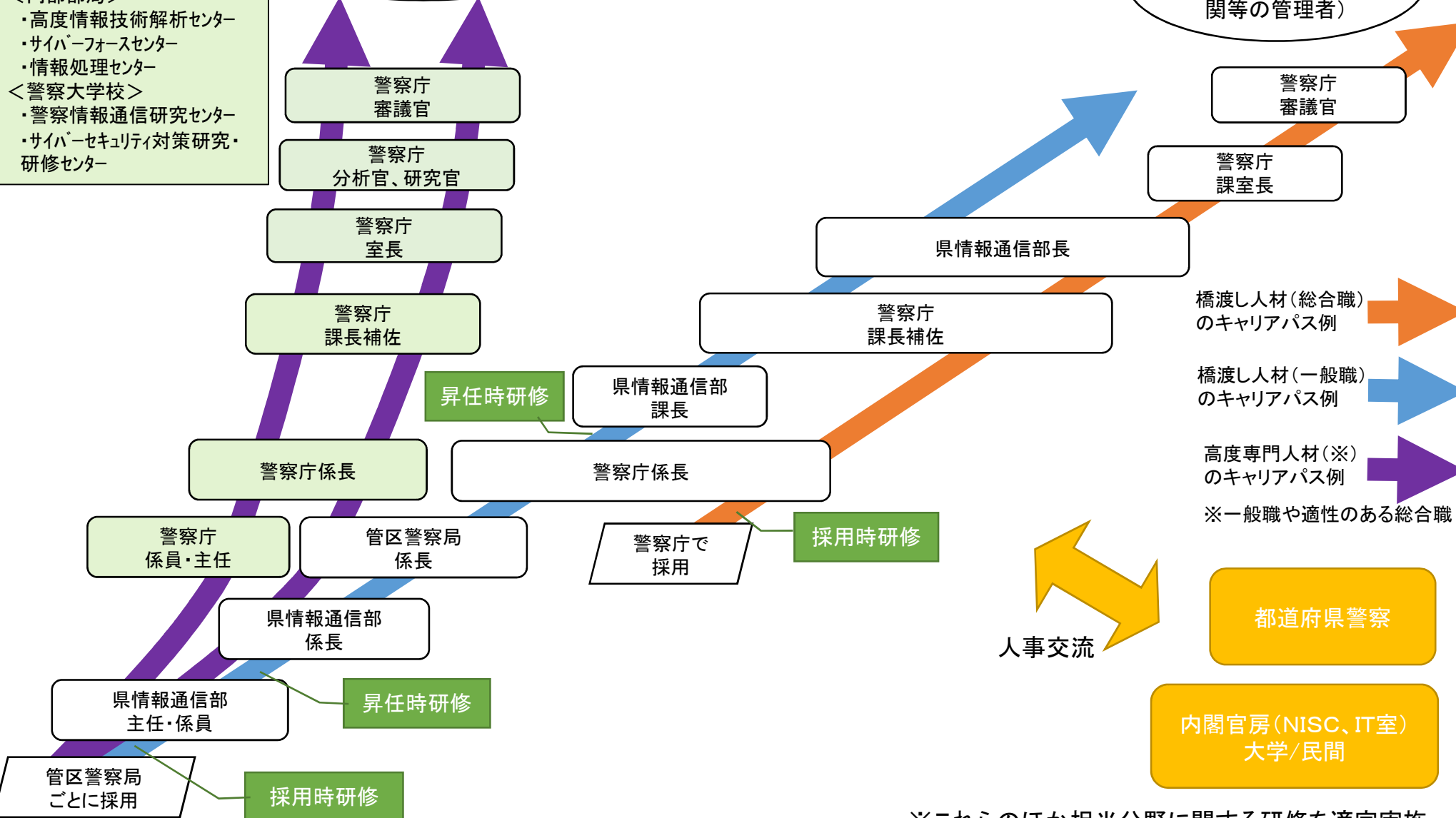
加えて、情報システムの取扱いやサイバー空間の脅威の情勢等に関する分かりやすい執務参考資料を作成し、職員へ配布するとともに、いつでも参照できるよう掲示板に掲載するなど、全警察職員の情報セキュリティ意識の醸成等を図る。

# 技術系職員のキャリアパスイメージ

警察庁における高度な実務を担当する部署  
 <内部部局>  
 ・高度情報技術解析センター  
 ・サイバーフォースセンター  
 ・情報処理センター  
 <警察大学校>  
 ・警察情報通信研究センター  
 ・サイバーセキュリティ対策研究・研修センター

高度専門人材  
 (高度な実務に従事する技術者)

橋渡し人材  
 (内部部局・地方機関等の管理者)



橋渡し人材(総合職)のキャリアパス例

橋渡し人材(一般職)のキャリアパス例

高度専門人材(※)のキャリアパス例  
 ※一般職や適性のある総合職

都道府県警察

内閣官房(NISC、IT室)  
 大学/民間

人事交流

※これらのほか担当分野に関する研修を適宜実施

# 個人情報保護委員会セキュリティ・IT人材確保・育成計画（概要）

平成 28 年 8 月 25 日

## はじめに

個人情報保護委員会（以下「委員会」という。）は、個人情報の適正な取扱いの確保を図ることを任務として平成 28 年 1 月に設置された、高い独立性を有する監視・監督機関である。具体的な業務として、マイナンバーの取扱いに係る監視・監督（マイナンバー法）及び個人情報の取扱いに関する監督（個人情報保護法）を行うほか、こうした業務を支えるための情報システムの整備・運用を行うものである。

このような監視・監督機関としての性格及び業務内容から、事務局職員のうち一定の職員には、セキュリティ・IT の知見が必要不可欠である。

そこで、委員会で所管する上記業務の適切な遂行及び情報システムの適切な整備・運用が、マイナンバーの適正な取扱いの確保及び個人情報の利活用・保護の推進のために必要不可欠であることを踏まえ、平成 31 年度を目途に、情報システムの適切な整備・運用とマイナンバーに係るセキュリティに関する監視・監督等を行う組織として、情報システム担当参事官以下の体制を整備し、その体制を担う人材としてセキュリティ・IT 人材の確保を図ることを目的に、以下のとおり「個人情報保護委員会におけるセキュリティ・IT 人材確保・育成計画」として策定するものである。

委員会では、本計画の着実な実施に向けて取り組むものとし、毎年度末にセキュリティ・IT 人材の確保・育成状況等をフォローするとともに、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

## 1. 体制の整備と人材の拡充

委員会では、セキュリティ・IT に係る統括部門（委員会内の情報システムの整備・運用の全体管理等）並びに上述の業務を適切に遂行するための部門（マイナンバーに係るセキュリティに関する監視・監督等）の体制の整備として、セキュリティ・IT 人材の確保を重視し必要な機構・定員要求を行う。また、人材の拡充及び能力の向上のために今後 4 年間において、新規採用職員を中心にセキュリティ・IT 関係の講座を有する大学及び大学院への派遣、諸外国の個人情報保護機関への派遣のほか、委員会事務局職員に対するセキュリティ・IT リテラシー等に関する研修の実施等を行う。

## 2. 有為な人材の確保

毎年度、一般職職員を 3～6 名程度新卒採用し、橋渡し人材候補として育成していくことを視野に入れた人材を確保する。その際、採用時の面接等で情報セキュリティや IT に係る素養及び関係業務への意向を確認することとする。新卒採用により確保

した人材については、出向、研修等を通じてセキュリティ・IT に関する能力等の育成、適正性の有無の判断等を行うものとする。

また、橋渡し人材については、最終的には新卒採用者からの育成を基本としつつ、当面はマイナンバーに係るセキュリティに関する監視・監督等業務におけるシステム面での分析関係業務に知見を有する人材の確保が必要であることから、民間企業等におけるセキュリティ・IT 関係業務に携わった経験のある者を必要に応じて任期付職員や非常勤職員、さらには中途採用職員として採用していく。なお、採用に当たっては、委員会における一般行政事務への志望のみならず、セキュリティ・IT 関係業務への意向及びこれまでに経験した業務内容や資格等を確認することとする。

### **3. セキュリティ・IT 人材育成支援プログラム**

委員会における「橋渡し人材」の候補者向けに、以下のとおり研修を実施する。

情報システムに関する研修については、総務省が実施する情報システム統一研修を活用し、委員会で新たに採用した職員は全員が、他府省からの出向職員は本人の知識及び技能の程度、保有する資格並びに業務上の必要性及び優先度を踏まえて受講することとし、併せて毎年のべ 40 名程度の受講を目途に実施するものとする。

情報セキュリティに関する研修については、情報システム統一研修（再掲）及び NISC 等が実施する研修を活用するとともに、委員会においても自ら研修等を行い、委員会で新たに採用した職員は全員が、他府省からの出向職員は本人の知識及び技能の程度、保有する資格並びに業務上の必要性及び優先度を踏まえて受講することとし、併せて毎年のべ 20 名程度の職員を対象に実施するものとする。

なお、情報セキュリティ責任者、課室情報セキュリティ責任者には、情報システム統一研修のうち「情報セキュリティ基礎」の受講を原則とする。

委員会では、情報システムの適切な整備・運用とマイナンバーに係るセキュリティに関する監視・監督等のために、セキュリティ・IT 及びマイナンバーについての知識・経験を有する者が必要である。他方、委員会で新たに採用した職員については、平成 27 年 4 月採用者（3 名）及び平成 28 年 4 月採用者（2 名）の計 5 名であり、係長級昇任時（5～6 年度メド）に、セキュリティ・IT に関する実践的な業務を経験させるために 1 名程度、類似の監督機関等に出向させることとする。

また、各府省から出向で派遣された職員を含めてセキュリティ・IT 関係の講座を有する大学及び大学院へ複数の職員を派遣する。平成 28 年度においては、将来の委員会を担う職員について、セキュリティ・IT 関係の大学院等での科目等履修を行うこととする。さらに、セキュリティ・IT 関係の業務を行っている監査法人等の民間企業への出向等についても、委員会で新たに採用する職員の採用状況等を踏まえて、将来的な実施の時期等を検討する。

#### 4. 人事ルート例（キャリアパスのイメージ）

##### (1) 全体的なキャリアパス像

委員会では、情報システムの適切な整備・運用とマイナンバーに係るセキュリティに関する監視・監督等の体制を整備し、必要な知識、経験を有する職員を確保・育成していくこととしている。こうした経験や知識・能力の習得の観点から、委員会事務局採用後に想定されるキャリアパスの一例は次のとおりである。

##### ◆採用・係員（採用年から5年目頃）

- ・研修：情報セキュリティ・ITに関する基礎的な研修
- ・所属部署：委員会事務局各係
- ・出向等：セキュリティ・IT関係の講座を有する  
大学及び大学院等での講座受講、海外執行機関等

##### ◆係長クラス（6年目頃）

- ・研修：情報セキュリティ・ITに関する実務的な研修
- ・所属部署：委員会事務局各係
- ・出向等：類似の監督機関等、海外執行機関等

##### ◆課長補佐クラス（15年目頃）

- ・研修：マネジメントに関する研修
- ・所属部署：委員会事務局各係
- ・出向等：類似の監督機関等、海外執行機関等

##### ◆管理職

- ・研修：マネジメントに関する研修
- ・所属部署：委員会事務局

##### (2) キャリアパスに含めることが想定される部署と役職

委員会において、情報システムやマイナンバーに係るセキュリティに関する監視・監督等に関係する部署として職員の配属が想定される部署・役職等は次のとおりである。

##### ① マイナンバーに係るセキュリティに関する監視・監督等に関する組織と役職

###### i) マイナンバー関係

事務局総務課（監視・監督担当）（企画官、補佐、係長）

事務局参事官室（システム担当）（参事官、企画官、補佐、係長）

###### ii) 個人情報の取扱い（①を除く）に係る監督に関する組織と役職

事務局参事官室（PD担当）（参事官、企画官、補佐、係長）

##### ② 情報システム・業務改革に関する組織と役職

i) 情報システム関係

事務局総務課（情報システム担当）（調査官、補佐、係長）

ii) 業務改革関係

事務局総務課（人事担当）（企画官、補佐、係長）

③ 一般行政事務について、特に経験をさせたい部署の業務及び想定される課室と  
役職

i) 事務局総務課（人事、会計といった内部管理業務）

- ・ 課長補佐（人事担当、会計担当）
- ・ 人事係長、会計係長

## 5. 一般職員の情報リテラシー向上

委員会は、個人情報 の適正な取扱いの確保を図ることを任務とする組織であることから、情報システムの整備・運用又はマイナンバーに係るセキュリティに関する監視・監督等業務に従事しない一般職員であっても、情報システム及び情報セキュリティに関する基本的な知識及び技能を習得して業務に従事することが不可欠である。このため、一般行政職員のリテラシー向上を図る観点から、次の研修を実施するものとする。

### ○新入職員・転入職員向け研修

- ・ 研修内容：情報セキュリティについて
- ・ 受講対象者：新入職員・転入職員
- ・ 実施時期：新入又は転入後なるべく速やかに
- ・ 実施方法：職員による講義形式

### ○全職員向け研修

- ・ 研修内容：情報セキュリティ研修
- ・ 受講対象者：全職員
- ・ 実施時期：随時（年数回）
- ・ 実施方法：職員又は外部講師による講義形式



金融庁

セキュリティ・IT人材確保・育成計画

**【概要版】**

平成28年8月31日

## 目次

はじめに .....	1
1. 体制の整備と人材の拡充 .....	2
2. 有為な人材の確保 .....	2
3. セキュリティ・IT人材育成支援プログラム .....	2
4. キャリアパス .....	3
(1) 金融庁におけるキャリアパス.....	3
(2) キャリアパスに含める部署と役職.....	4
① セキュリティについて経験できる課室と役職.....	4
② 情報システム・業務改革について経験できる課室と役職.....	4
5. 職員の情報リテラシー向上 .....	4

## はじめに

行政機関の情報システムについては、行政運営の重要な基盤をなすものであり、情報通信技術を活用し、行政運営の効率性や行政サービスの利便性の向上を実現していくことが重要な課題である。また、標的型メール攻撃やDDoS攻撃等に見られるように、情報の搾取や業務の遂行を脅かすことを企図したサイバー攻撃の脅威が高まっており、サイバーセキュリティ対策をさらに強化していくことも喫緊の課題となっている。

このため、金融庁においては、情報システムの整備及び運用に関しては、政府共通ルールに基づき、ITガバナンスの強化に努めている。また、サイバーセキュリティに関しても、リスクを網羅的に評価・把握し、必要な対策を順次実施し、セキュリティ水準の向上に取り組んできているところである。

さらに、サイバーセキュリティに関しては、金融庁の所管する金融分野においても、サイバー攻撃により金融機関や金融市場インフラの機能が停止する等のリスクが増大しており、サイバーセキュリティの確保は、金融システム全体の安定のための喫緊の課題であるため、官民一体となって金融システム全体の強靱性の向上に取り組んでいる。

金融庁としては、こうした取組みを進める体制強化に努めてきているところであるが、体制を担う情報技術やセキュリティに関する知識・経験を有する人材が、いまだ十分ではない現状に鑑み、更なる強化を図ること目的として、以下のとおり、「金融庁におけるセキュリティ・IT人材確保・育成計画」を策定した。今後、本計画の着実な実施に向けて取り組むものとし、セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、見直しを行うものとする。

## **1. 体制の整備と人材の拡充**

サイバーセキュリティ（金融分野のサイバーセキュリティを含む。以下同じ。）及びITに係る統括部局、社会的に影響の大きい重要システムを所管する部局について、情報システムの適切な運用管理及びセキュリティ対策を実施する上で必要な体制を整備するための機構・定員要求を行う。

また、セキュリティ・IT人材の拡充及び能力向上のため、職員の内閣サイバーセキュリティセンター（以下、「NISC」という。）などの政府機関への出向、官民人事交流法及び任期付職員法を活用した外部人材の登用、IT大学院への派遣、金融庁及び外部機関の実施する基礎的・専門的な研修受講の奨励等を行う。

## **2. 有為な人材の確保**

セキュリティに関して対応が求められる事案の急増、情報システムによる更なる業務効率化の推進など、セキュリティ・ITに係る業務の増加、複雑困難化がみられる中では、セキュリティ・ITに関する一定の専門性と、金融行政に関する十分な知識・経験を有し、セキュリティ・IT高度専門人材と一般行政部門との橋渡しをする人材を確保・育成していくことが必要である。

このため、新規採用において、橋渡し人材候補者として育成していくことを視野に入れた人材を一定程度確保していく。新規採用により確保した人材については、専門知識の習得や実務経験を積みながら、適性の有無の判断を行うものとする。

また、セキュリティ・ITに関心のある職員や中途採用者に関しても、橋渡し人材の候補者として、セキュリティ・IT関係部署でのOJTや関係する研修等を通じて専門知識の習得度を確認しながら、適性の有無を判断するものとする。

## **3. セキュリティ・IT人材育成支援プログラム**

セキュリティ・IT人材の育成については、適性のある人材を発掘・確保・育成しつつ、優良な人材が将来にわたって、活躍できる環境を整備していく必要がある。

具体的には、新規採用者やセキュリティ・ITに関心のある職員に関して、金融庁及び外部機関の実施する基礎的・専門的な研修の受講、NISCなど政府機関への出向、セキュリティベンダーやIT企業への派遣、IT大学院への派遣について、引き続き実施していく。

なお、政府機関や民間企業への出向、IT大学院への派遣に関しては、セキュリティ・IT人材の育成における重要なキャリアパスとして位置付けるとともに、出向・派遣の経験者が、金融庁内において指導的な立場に立ち、それまでに培った豊富な知識・経験等を伝授していくことにより、金融庁全体の人材の底上げを図る。

また、金融資本市場及び金融業界の保有する情報には極めて高いセキュリティが求められることなどに鑑み、それらを所管する金融庁としては、セキュリティ・IT人材育成のための新たな方策として、サイバーセキュリティ分野の世界最先端で活躍する外部専門家を招聘して指導・助言を仰ぐ環境を整えるなど、人材育成に一層注力する。

## 4. キャリアパス

### (1) 金融庁におけるキャリアパス

金融庁では、サイバーセキュリティ対策や情報システムの適切な運用管理について、必要な知識、経験を有する職員を確保・育成していくこととし、職員の階層に応じたキャリアパスの一例は、次のとおり。

#### ◆採用・係員（採用年～6年目頃）

研修 : IT基礎知識研修【ITパスポート試験相当】  
所属部署 : 総務企画局総務課情報化統括室  
出向等 : IT大学院

#### ◆係長クラス（7～15年目頃）

研修 : 情報セキュリティマネジメント研修【情報セキュリティマネジメント試験相当】  
所属部署 : 検査局総務課金融証券検査官（システムモニタリングチーム）  
出向等 : 民間企業（セキュリティベンダー、IT企業）

#### ◆課長補佐クラス（16～30年目頃）

研修 : 最新動向、先端ケーススタディを取り入れた演習  
所属部署 : 総務企画局政策課課長補佐（サイバーセキュリティ対策企画調整室）  
出向等 : NISC

#### ◆管理職（31年目頃以降）

研修 : 外部セミナー  
所属部署 : 総務企画局総務課情報化統括室長  
出向等 : IT総合戦略室

◆審議官（サイバーセキュリティ担当）

研修：サイバーセキュリティ・情報化審議官等研修

(2) キャリアパスに含める部署と役職

金融庁において、サイバーセキュリティ対策や情報システムに関係する部署として、職員の配属が想定される部署・役職等の一例は、次のとおり。

① セキュリティについて経験できる課室と役職

総務企画局政策課サイバーセキュリティ対策企画調整室

- ・サイバーセキュリティ対策企画調整室長
- ・課長補佐（サイバーセキュリティ対策担当）
- ・サイバーセキュリティ対策係長

② 情報システム・業務改革について経験できる課室と役職

総務企画局総務課情報化統括室

- ・情報化統括室長
- ・情報企画調整官
- ・課長補佐（情報化推進業務企画係担当）
- ・課長補佐（情報化技術係担当）
- ・情報化推進業務企画係長
- ・情報化技術係長

## 5. 職員の情報リテラシー向上

金融庁においては、全職員を対象として、セキュリティ・ITに関する知識の付与を目的とした研修を実施するほか、幹部職員を対象とした研修の実施により、職員の情報リテラシーの向上を図る。

① 全職員向け研修

イ. 情報管理研修（必修）

- ・目的：情報セキュリティに関する基本的知識の付与
- ・受講対象者：全職員
- ・受講予定者数：毎年1,700名程度
- ・実施時期：4月、7月、8月、10月、1月

- ・実施方法：講義形式

ロ. IT・セキュリティ研修（必修）

- ・目的：職員のITリテラシーの向上
- ・受講対象者：全職員
- ・受講予定者数：毎年1,700名程度
- ・実施時期：4月、8月、12月
- ・実施方法：講義形式

② 個室幹部向け研修

イ. 情報管理研修

- ・目的：情報セキュリティに関し、特に組織のトップマネジメント層として必要な知識の付与
- ・受講対象者：個室幹部
- ・受講予定者数：毎年30名程度
- ・実施時期：10月
- ・実施方法：講義形式

③ 新規採用職員研修

イ. IT基礎知識に係る講義

- ・目的：ITパスポート取得相当の知識の付与
- ・受講対象者：新規採用職員（一般職）※必修
- ・受講予定者数：毎年30名程度
- ・実施時期：9月～10月
- ・実施方法：講義形式

（以 上）

# 【概要】 〔消費者庁〕 セキュリティ・IT人材確保・育成計画

## (1) 背景・目的

- 「政府機関におけるセキュリティ・IT人材育成総合強化方針(平成28年3月決定)」に基づき、全府省庁が計画を作成
- サイバーセキュリティ対策と情報システムの適切な運用・管理における「人材の確保や育成を図る」体制を確実に整備
- 消費者庁で所管する情報システムの実情や組織の特性を踏まえ、将来にわたる具体的な取組方策を策定

## (2) 計画期間

- 平成28年度から平成31年度までの4か年を目途  
毎年度、本計画のフォローアップを行い、必要に応じて適切かつ柔軟に計画の見直しを実施

## (3) 消費者庁の特性

- 組織規模、予算、執行体制等
  - ・ 消費者庁の職員数は全府省庁の中でも比較的小規模  
職員構成は「他府省庁からの出向者」、「任期付職員」や「政策調査員」等が多数、「消費者庁新規採用職員」は少数
  - ・ 情報システム関連については、担当職員数、予算額や保有システム数ともに全府省庁の中でも非常に小規模
  - ・ 計画期間内に「消費者庁LANシステムの更改」を予定しており、円滑な移行に向けて体制の拡充が不可欠

## (4) 計画の推進体制

- 消費者庁における推進体制  
計画を着実に推進するため、消費者庁参事官の下で人事部門とシステム部門等が連携して評価・検討、見直しを実施
- 政府内での推進方法  
セキュリティ・IT人材確保・育成計画は、各府省庁情報化専任審議官等連絡会議で共有を行い、フォローアップを実施



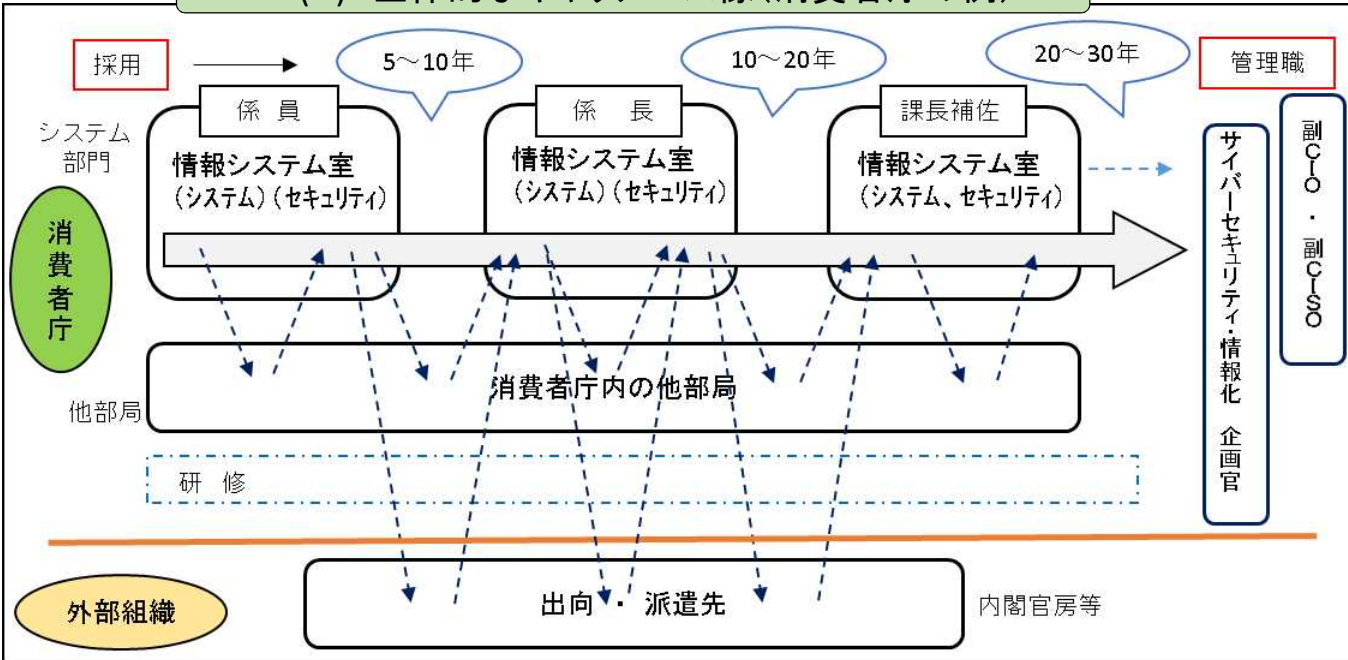
(5) 項目別の実施内容

項 目	計 画 内 容
<p>1. 体制の整備</p> <p>(1)システムの統括部局</p> <p>(2)社会的な影響の大きいシステムを所管する部局</p>	<ul style="list-style-type: none"> <li>・平成29年度定員要求を行い、セキュリティ担当を中心に増員を図り組織体制を強化</li> <li>・今後の状況等の変化を考慮しつつ必要となれば、組織体制について適切に対応</li> </ul>
<p>2. 有為な人材の確保</p> <p>(1)新規採用職員</p> <p>(2)中途採用職員等</p>	<ul style="list-style-type: none"> <li>・行政職等で採用された新規職員のうち、セキュリティ・IT部門への定期的な配置を検討</li> <li>・「中途採用」や「任期付採用」で専門知識・実践経験豊富な即戦力人材の採用を検討</li> </ul>
<p>3. 人材育成支援プログラム</p> <p>(1)研修</p> <p>①内閣官房・総務省の研修</p> <p>②消費者庁が自ら実施する研修</p> <p>(2)出向等</p> <p>①政府機関への出向</p> <p>②国内外の大学院等への派遣</p> <p>③民間企業への派遣</p>	<ul style="list-style-type: none"> <li>・内閣官房(NISC)、総務省等が実施する研修(情報システム統一研修等)を積極的に活用</li> <li>・組織が小規模なため、必要な場合は他省庁との合同開催も検討</li> <li>・政府機関(内閣官房等)への出向・人事交流の実現を目指す</li> <li>・職員数が少なく人材が限られていることから、在外研究員等の派遣は困難</li> <li>・職員数が少なく人材が限られていることから、民間企業への派遣は困難</li> </ul>

(5) 項目別の実施内容〔続き〕

項目	計画内容
4. 人事ルート (キャリアパスのイメージ) (1) 全体的なキャリアパス像 (2) 部署と役職	<ul style="list-style-type: none"> <li>・人事ルートのイメージを想定 (下記の左図を参照)</li> <li>・経験が望ましい配置を想定 (下記の右上を参照)</li> </ul>
5. 一般職員の情報リテラシーの向上	<ul style="list-style-type: none"> <li>・消費者庁職員向けの研修・訓練の開催 (下記の右下を参照)</li> </ul>

4. (1) 全体的なキャリアパス像(消費者庁の例)



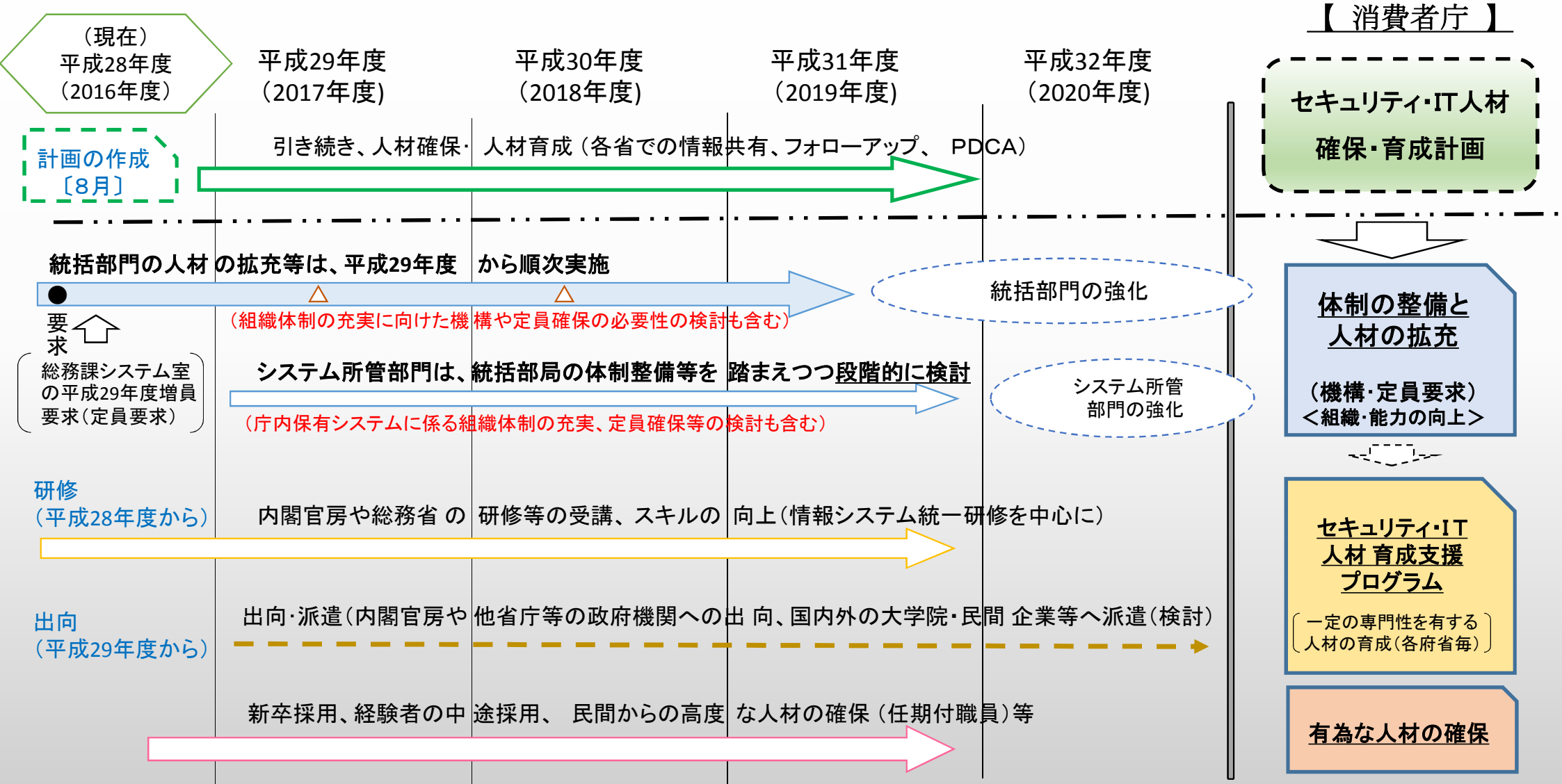
4. (2) 部署・役職

- セキュリティ・情報システム・業務改革等を担当 総務課 (企画官、課長補佐、係長)
- 国民生活センターを所管している部署 消費者教育・地方協力課 (課長補佐、係長)
- 調達業務、予算業務、消費者政策(情報通信)、等 庁内の関係各課 (課長補佐、係長)

5. 一般職員の情報リテラシー向上

消費者庁では 一般行政職員の情報リテラシー向上 のため 情報システム・セキュリティに関する研修を実施中

- 全職員向け研修 : 情報セキュリティ研修 (e-ラーニング)
- 新規採用職員向け研修の一部 : セキュリティ、個人情報
- 新規転入職員向け研修の一部 : セキュリティ、個人情報
- 全職員 : 標的型メール訓練 (不審メールの対応)



# 復興庁におけるセキュリティ・IT人材確保・育成計画【概要版】

平成 28 年 8 月 31 日

## ●はじめに

本計画は、復興庁の組織の特殊性を鑑み、復興庁が所管する情報システムの適切な運用管理とサイバーセキュリティ対策を切れ目なく継続的に実施するための体制の強化を図るため、平成 29 年度を目途に、サイバーセキュリティ・情報化を担当する職員の体制を強化し、その体制を担う人材の確保・育成を図ることを目的に、以下のとおり「復興庁におけるセキュリティ・IT人材確保・育成計画」として策定したものである。

復興庁では、本計画の着実な実施に向けて取り組むものとし、セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

## ●体制の整備と人材の拡充

復興庁では、セキュリティ・ITにかかると統括担当部局の職員体制の整備として、サイバーセキュリティ対策を切れ目なく継続的に実施するための体制の確保に向け、必要な機構・定員要求を行う。また、復興庁においてサイバーセキュリティ・情報化に関する業務に従事する職員に対し、セキュリティ・ITに関する研修へ積極的に参加させることにより、人材の拡充を図ることとする。

## ●セキュリティ・IT人材育成支援プログラム

復興庁においてサイバーセキュリティ・情報化に関する業務に従事する職員に対し、総務省が主催する情報システム統一研修に参加させるなど、当該業務に従事する職員の能力の向上を図っていく。

## ●一般職員の情報リテラシー向上

復興庁では、セキュリティ・ITに関する一般職員の情報リテラシー向上のため、以下の研修を実施する。

### ○全職員向け研修

- ・研修内容：情報セキュリティ関係規程、情報セキュリティ対策等の理解
- ・受講対象者：全職員
- ・受講予定者数：毎年 500 名程度
- ・実施時期：毎年 5～6 月頃
- ・実施方法：講義形式

### ○転入者向け研修

- ・研修内容：情報セキュリティ関係規程、情報セキュリティ対策等の理解
- ・受講対象者：新規転入者

- ・受講予定者数：毎年 100 名程度
- ・実施時期：随時
- ・実施方法：講義形式又は個別形式

○課室情報セキュリティ責任者向け研修

- ・研修内容：情報セキュリティに係る責任者の責務と役割
- ・受講対象者：課室情報セキュリティ責任者
- ・受講予定者数：毎年度 30 名程度
- ・実施時期：毎年 5～6 月頃
- ・実施方法：講義形式

○全職員向け標的型攻撃メールに対する教育訓練

- ・訓練内容：標的型攻撃の模擬メールを受信した職員の対応確認
- ・訓練対象者：全職員
- ・訓練想定数：毎年 500 名程度
- ・訓練時期：年 3 回程度
- ・実施方法：外部委託

# 総務省サイバーセキュリティ・IT人材確保・育成計画概要

平成 28 年 8 月 31 日  
情報化統括責任者  
最高情報セキュリティ責任者  
大臣官房長

## はじめに

総務省においては、平成 19 年度の「行政機関における IT 人材の育成・確保指針」（平成 19 年 4 月 13 日 CIO 連絡会議）、同 20 年度の「電子政府推進計画」（平成 20 年 12 月 25 日 CIO 連絡会議）等を受け、「総務省電子政府推進計画」（平成 20 年 3 月 28 日総務省行政情報化推進委員会）及び「総務省行政 ICT 化推進計画」（平成 28 年 4 月 15 日総務省行政情報化推進委員会改定）を策定し、行政 ICT 化の更なる推進とともに、「総務省情報セキュリティポリシー」（平成 28 年 4 月 15 日総務省行政情報化推進委員会改定）を策定するなどサイバーセキュリティ対策を通じて安全・安心な ICT 環境や体制・人材の充実強化に向け、着実に取り組んできたところである。

政府全体を巡る状況としては、平成 27 年に日本年金機構において、標的型メール攻撃によって大量の個人情報流出する事案の発生等外部からの攻撃が増加し、厳しさを増している。また、平成 29 年マイナンバー（社会保障・税番号）制度の情報連携開始に向け、安定的な運用やセキュリティの確保が急務となっている。そうした中、今般、政府全体の方針として、「サイバーセキュリティ人材育成総合強化方針」（平成 28 年 3 月 31 日サイバーセキュリティ戦略本部）が策定されたことを受け、省内外の一般行政を支え、国民サービスの提供の基盤となる情報システムを所管する総務省においても、以下のとおり「総務省サイバーセキュリティ・IT人材確保・育成計画」を策定する。本計画においては、平成 28 年度から平成 31 年度の 4 年間を見据え、今後の展望や研修等の充実に向けた具体的な取組方針について示すこととする。

なお、本計画については、サイバーセキュリティ・IT人材の確保・育成に関する進捗等を踏まえ、必要に応じて結果を評価し、PDCA サイクルに基づき、適切かつ柔軟に見直しを行っていくこととする。

## 1. 体制の整備と人材の拡充

総務省は、行政運営の改善、地方行財政、情報通信など、国家の基本的仕組みに関わる諸制度を支える社会的に影響の大きいシステムを所管しており、このような重要なシステムについては、安定性・継続性のある管理・運用が不可欠である。また、内閣官房情報通信技術総合戦略室や内閣官房内閣サイバーセキュリティセンターと連携しつつ、政府全体の ICT 化、サイバーセキュリティの確保、業務改革等に係る施策を推進するという制度官庁としての役割も有している。

総務省においては、従前より CIO 補佐官や最高情報セキュリティアドバイザーを活用し、

行政の情報化及びサイバーセキュリティの確保のための取組を行ってきたところである。それに加え、今後全体の体制整備を行うことに先行して平成 28 年度からサイバーセキュリティ・情報化審議官を設置したが、当該審議官の司令塔機能・統括機能を十分に支えるべき統括部局の体制は未だ整備されておらず、司令塔機能・統括機能については、サイバーセキュリティ・情報化審議官に就く職員の知見等に依存した体制となっているのが現状である。また、システム所管部局においても技術の進歩等により今後更に高度化・増加すると予想される業務に対応していく上では、人材の確保・育成や更なる体制の強化が課題となる。

このため、統括部局及びシステム所管部局について、必要な機構・定員要求を行うとともに、情報システムの企画・管理・運用やサイバーセキュリティに関する専門知識を有するだけでなく一般行政全般に係る知識・能力を有し、意思決定を行う者を技術面・実務面から適切にサポートできる職員（以下、「橋渡し人材」という。）をも十分に確保・育成していくため、採用活動や研修プログラムの充実を図る。あわせて、一般職員についても、その役割に応じた知識・経験を有していることが求められるため、総務省職員として必要な情報システム及びサイバーセキュリティに係る基本的事項について研修を行い、省全体としてのレベル向上を図ることとする。

また、統括部局及びシステム所管部局双方での企画・管理・運用業務の経験、他府省への職員の出向、民間企業（サイバーセキュリティ・ICT 関係企業等）との人事交流等を継続して実施することにより、より実践的な知識・経験を有する人材の育成に努めていく。

#### （１）サイバーセキュリティ・ITに係る統括部局の体制の整備

総務省においては、まず平成 29 年度から PMO たる大臣官房企画課情報システム室及び政府全体の電子化を担う行政管理局において体制の整備を図り、同 30 年度以降に緊急度の高い情報システムを所管する部局から順に体制の整備を図る。

#### （２）社会的な影響の大きいシステムを所管する部局の体制の整備

#### （３）人材の拡充についての方針

今後、「1」のとおり所要の体制を整備するとともに、安定的かつ恒常的に有為な人材の確保・育成を目指すこととする。具体的には、現状では情報システム部門の業務は一部の当該部門での経験が長期に渡る職員に集中する傾向にある。一方で、当該部門での経験が浅い職員は情報システム部門に配属されても今後長期にわたって当該部門で登用されることを想定せず、資格の取得や研修の受講等積極的な能力向上へのインセンティブが十分でないのが現状である。そこで、幅広い職員が情報システム分野に配属されるとともに、その後も計画的に情報システム分野とその他部門を交互に経験させ、情報システム部門で得られた知見や能力が人事ローテーションの中で発揮されるよう配慮する。くわえて、そのような取組を広く省内職員に周知することで、当該部門に配属された職員の資格や研修へのモチベーションの向上を図り、当該部門の知識と一般行政に対する知識を併せ持つ職員の確保に努める。あわせて、採用についてはサイバーセキュリティや ICT に係る素養及

び関係業務への意向を意識した採用活動を行うほか、必要な研修の実施等を通じ、総務省における人材の拡充を図ることとする。

このような取組を通して、目標とすべき職員のスキルレベルの例を以下に示す。

(情報システム所管部局及び統括部門の幹部職員)

- ・ ICT に関する最新の動向や知見を有し、省内システムに対して適切な指導・助言ができる者
- ・ サイバーセキュリティマネジメントに精通し、サイバーインシデント発生時に、適切な判断・指示が行える者

(上記両部門の担当職員レベル)

- ・ システムに関する知識を十分に持ち、システムの企画・管理・運用に当たり、委託先企業職員とも対等に議論ができる者
- ・ サイバーセキュリティに関する知識を持ち、サイバーインシデントの未然防止、発生時の適切な対処が行える者

(その他部局も含めた一般職員)

- ・ 職業人が共通に備えておくべき ICT に関する基礎的な知識を有する人材

## 2. 有為な人材の確保

総務省においては、橋渡し人材について、現在抱える職員については、今後の人事ローテーションや出向、研修等を通じて確保・育成していくこととするが、あわせて、新規採用の場においても確保・育成に努める。

この点において、総務省としては従来より、既に情報通信部門等において採用時点で、技術面を重視した人材の確保を行っているが、これとは別に、毎年度、採用時の面接等でサイバーセキュリティや ICT に係る素養及び関係業務への意向が確認できた者を、定員の枠内で 1～2 名程度を情報システム及びサイバーセキュリティ分野における橋渡し人材候補として採用する。

採用により確保した人材については、計画的に内閣官房情報通信技術総合戦略室や内閣官房内閣サイバーセキュリティセンターといった他府省の情報部門へ出向させたり、研修への参加を促す。また、その他の職員について、通常業務の過程で情報システム関係業務への素養が認められたり、人事面談等適宜のタイミングで関係業務への意向が確認されたりした場合には、情報部門での育成に重点を置くことを可能とする。

## 3. サイバーセキュリティ・IT 人材育成支援プログラム

総務省では、橋渡し人材の育成に関する研修について、セキュリティ対策、システム企画・管理・運用について様々なスキルを身につけるため、原則として内閣官房や総務省行政管理局による研修プログラムを活用し、平成 27 年度受講実績 138 名程度のうち、受講者が比較的少ない A コース及び C コース以上に重点を置き、更に拡大していく。

具体的には、まず、係員時に受講することを想定している A レベルの研修について、現状では受講者数が 14 人（昨年度実績）と、B レベルの 76 名（同左）と比較して少なくな



っているが、これは下記に示すとおり、提供するコース数の違いもあるが、それ以外にも、情報部門に配属になった時点で、配属された部局の業務の特殊性を考慮し、分野ごとに分けられた B レベルの各研修から受講を開始しているパターンが多いことが理由の一つとして考えられる。一方で、A レベルの研修内容は、情報システムやセキュリティを扱う総務省職員として最低限身につけておくべきものであり、今後、業務に必要な情報分野の応用的知識を身につける際の前提として、職員の採用時に一律に受講させることとする。

また、係長以上で受講することを想定している C レベル以上のコースもレベルが上がっていくごとに受講者の減少が見られる。この理由として、B レベルの研修を配属時に受講し（又はしていない場合も）、業務による受講時間の確保が困難であったり、業務上最低限必要な知識は OJT で身についたと考えられたりしている点が考えられる。しかし、これらのレベルの研修もその役職や在籍年数に応じ、必要な知識や技法が習得できるものであり、特に情報システム・セキュリティに関わる職員は係長在任時に受講を完了することとし、最終的には課長補佐クラスになる前に、D レベルのコースのうち、業務の特性を鑑み、情報システムの運用・保守やサイバーセキュリティ等についてそれぞれ必要なものの受講が完了していることとし、周知及び受講を促進する。詳しくは以下に記すとおりである。

## (1) 研修

### ①内閣官房及び総務省において用意する研修の活用

○今後の目標（当該レベル研修を受講完了している職員数。）

レベル	A	B	C	D1	D2
コース数	1	3	2	4	5
①今後4年間の各年度目標人数（全体）	50名程度	100名程度	40名程度	20名程度	20名程度
②①のうち、橋渡し人材又はその候補となる職員の目標人数	35名程度	70名程度	30名程度	15名程度	15名程度

※各レベルの目安については、研修提供部門で設定するもの。以下のとおり。

A：情報システム部門に初めて配属となった時点又は橋渡し人材候補となった時点（採用時を含む）で受講するレベル

B：ITパスポートレベル

C：基本情報技術者、セキュリティマネジメントレベル

D1：応用情報技術者レベル

D2：上級（標準ガイドライン等の内容を受講可能な）レベル

## ○平成 27 年度実績

レベル	A	B	C	D1	D2
人数	14 名	76 名	34 名	10 名	4 名

## ②総務省において自ら実施する研修等

### ○情報システム研修会

- ・ 研修内容 : 情報システムのライフサイクル（企画、設計・開発、運用）に応じて情報システム担当職員が行うべき事項について
- ・ 受講対象者 : 情報システム担当職員
- ・ 昨年度受講者実績 : 68 名
- ・ 実施時期 : 随時（年間 6 回程度）
- ・ 実施方法 : CIO 補佐官、最高情報セキュリティアドバイザーによる講義形式

## （２）出向等

総務省は、前述のとおり社会的に影響の大きいシステムを所管する部局を有することに加え、政府全体の電子化を担う行政管理局を有することもあり、従来からサイバーセキュリティや ICT に関する専門知識や政策において幅広く知識を有する職員が関係機関に出向することで、当該機関の業務に貢献するとともに、継続的にこうした人材を確保・育成するため、内閣官房情報通信技術総合戦略室、内閣官房内閣サイバーセキュリティセンター、個人情報保護委員会事務局といった他府省の情報部門への職員の派遣を積極的に行っている。これにより、当該職員について、関係業務への知識・経験が身につくだけでなく、出向を終えた職員が再び省内情報部門に復帰した際には、出向経験のある他府省の情報部門との連携がスムーズになるなど、付随した効果も想定されるため、今後も職員数の拡大を図るとともに、他府省に加え、国立研究開発法人情報通信研究機構やサイバーセキュリティ関連民間企業への出向等を、様々な職員が経験できるよう配慮する。

## 4. 人事ルート例（キャリアパスのイメージ）

### （１）全体的なキャリアパス像

総務省では、情報システムの適切な企画・運用・管理とサイバーセキュリティ対策の指揮監督する体制を整備し、必要な知識、経験を有する職員を確保・育成していくこととしている。こうした情報システムやサイバーセキュリティ対策に関係する経験や知識・能力の習得の観点から、総務省採用後に想定されるキャリアパスの一例は次の通りである。

### ◆採用・係員（採用から 7 年目途）

- ・ 研修 : 情報システム統一研修（A～B レベル）及び情報システム研修会の受講
- ・ 所属部署 : 大臣官房企画課ほか情報システム関係部局係員

### ▶係長クラス（採用から 8 年以降）

- ・ 研修 : 情報システム統一研修（C～D レベル）の受講

- ・所属部署：大臣官房企画課ほか情報システム関係部局係長・主査・専門職
- ・出 向：内閣官房情報通信技術総合戦略室や個人情報保護委員会事務局、内閣官房内閣サイバーセキュリティセンターの係長・主査等

◆課長補佐クラス（採用から15年以降）

- ・所属部署：大臣官房企画課ほか情報システム関係部局課長補佐・専門官
- ・出 向：内閣官房情報通信技術総合戦略室や個人情報保護委員会事務局、内閣官房内閣サイバーセキュリティセンターの参事官補佐等

◆管理職（適性に応じて）

- ・所属部署：情報システム関係部局室長・課長
- ・出 向：内閣官房情報通信技術総合戦略室や個人情報保護委員会事務局、内閣官房内閣サイバーセキュリティセンターの参事官や企画官等

◆サイバーセキュリティ・情報化審議官

- ・研 修：サイバーセキュリティ・情報化審議官等研修

（2）キャリアパスに含めることが想定される部署と役職

総務省において、情報システムやサイバーセキュリティ対策に関係する部署として職員の配属が想定される部署・役職等は次の通りである。

①セキュリティについて経験することが想定される課室と役職

i) 大臣官房企画課情報システム室・同個人番号企画室

- ・室長
- ・課長補佐
- ・係長

ii) 情報流通行政局情報流通振興課情報セキュリティ対策室

- ・室長
- ・課長補佐
- ・係長

iii) 行政管理局行政情報システム企画課・行政情報システム管理室

- ・課長補佐
- ・係長

iv) 行政管理局管理官室(業務・システム改革総括、情報システム班)

- ・副管理官
- ・主査

v) 総合通信基盤局電波利用料企画室(システム計画係・運用係)

- ・室長
- ・補佐
- ・係長

- ・ 担当官

②情報システム・業務改革について経験することが想定される課室と役職

i) 大臣官房企画課情報システム室・同個人番号企画室

- ・ 室長
- ・ 課長補佐
- ・ 係長

ii) 行政管理局管理官室(業務・システム改革総括、情報システム班)

- ・ 副管理官
- ・ 主査

iii) 総合通信基盤局電波利用料企画室(システム計画係・運用係)

- ・ 室長
- ・ 補佐
- ・ 係長
- ・ 担当官

③事案対処、保安、事故対応、危機管理、安全保障等について経験することが想定される課室と役職

i) 大臣官房総務課

ii) 消防庁

## 5. 一般職員の情報リテラシー向上

行政の ICT 化及びサイバーセキュリティの確保については、情報システムを所管する部門や省の統括部門においてのみの人材の確保・育成では不十分であり、一般職員においても、日々の業務において利用できるシステムの機能について理解し、サイバーセキュリティについて高い意識を持つことが、効率的かつ安全な行政運営のために重要である。特に、サイバーセキュリティについては、日常的な業務で利用するインターネットの閲覧やメールの使用にも、マルウェア感染等の危険は潜んでおり、防止のための取組、万一感染が確認された場合の対応など身につけるべき知識は多くある。そこで、総務省では、情報システム及びサイバーセキュリティに関する一般行政職員のリテラシー向上のため、今後も次の研修を実施する。

### ○総務省情報セキュリティポリシー教育・自己点検

- ・ 研修内容 : 情報セキュリティについて、総務省職員として遵守すべき基本的事項について
- ・ 受講対象者 : 政務等を除く全職員
- ・ 実施時期 : 毎年 10~12 月頃
- ・ 実施方法 : e-learning

○新規採用職員への研修

- ・ 研修内容 : 総務省職員として、業務上利用するシステム及びサイバーセキュリティに関する基本的事項
- ・ 対象者 : 各年度新規採用職員
- ・ 実施時期 : 毎年 1 回
- ・ 実施方法 : 採用時におけるその他研修と同様に、座学で実施

## 法務省におけるセキュリティ・IT人材確保・育成計画（概要版）

### はじめに

今日、法務省が担うべき施策は、観光立国実現に向けた出入国手続の迅速化・円滑化，世界一安全な日本創造のための再犯防止対策の強化，震災復興支援や社会保障・税に関わる番号制度への対応等のための登記インフラの充実を始めとして，国民生活に密接に関連する広範な分野に及び，法務行政が果たすべき使命は，ますます重要なものとなっている。他方，政府機関を標的とするサイバー攻撃が増加するなど，セキュリティリスクが急激に高まってきており，これらの重要な施策を遂行するためには，土台となる情報システムの適切な運用管理及びセキュリティ対策の総合的な強化に向けた取組が必要不可欠であることから，法務省においては，「平成28年度法務省対策推進計画」を策定し，重点的に取り組んでいるところである。

これらの対策を着実に実施するとともに，セキュリティ対策と一体となった業務改革（BPR）を推進していくためには，セキュリティ・ITに係る業務を担う人材の確保・育成が重要であるが，法務省においては，各組織の所掌業務がそれぞれ高度の専門性・特殊性等を有し，それら所掌業務を担う職員の採用・人事管理は各組織ごとに行っていることもあって，セキュリティ・ITに係る有為な人材の確保及び中長期的な計画に基づく人材育成は必ずしも十分になされてこなかったきらいがある。

こうした課題に対処するため，法務省においては，先般，政府全体の方針として策定された「サイバーセキュリティ人材育成総合強化方針」（平成28年3月31日サイバーセキュリティ戦略本部決定）（以下「総合強化方針」という。）にのっとり，本計画を策定することとした。

本計画は，法務省所管の情報システムが，法務行政の遂行を支える重要な要素であることを踏まえ，当該情報システム及び情報をセキュリティ・リスクから保護し，かつ，効率的な行政運営の実現を図るため，情報システムの適切な運用管理及びサイバーセキュリティ対策を強化するための体制を整備するとともに，情報セキュリティインシデントに対処するために設置した法務省CSIRT（Computer Security Incident Response Team）の機能を強化し，セキュリティ・IT体制全般を担う人材として「橋渡し人材」<sup>(※)</sup>の確保・育成を図ることを目的として策定したものである。

法務省においては，平成32年3月31日までを計画期間として，本計画の着実な実施に向けて取り組むとともに，セキュリティ・IT人材の確保・育成状況等を踏まえ，必要に応じて，適切かつ柔軟に本計画の見直しを行っていくこととする。

---

(※) セキュリティ・ITに関する一定の専門性と法務行政に関する十分な知識・経験を有し，高度専門人材と一般行政部門との橋渡しをする人材のこと。

## 1 体制の整備と人材の拡充

法務省では、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等に関して、平成28年度から、最高責任者である情報化統括責任者（CIO）及び最高情報セキュリティ責任者（CISO）を補佐し、省内全体を指揮監督できるサイバーセキュリティ・情報化審議官を設置したことを踏まえ、同審議官を情報化統括・情報セキュリティ副責任者（副CIO・CISO）にするとともに、法務省CSIRTの運用責任者に指名し、体制の強化を図ったところである。

また、サイバー攻撃の高度化・巧妙化により、セキュリティ・ITに係るリスクが深刻化する中、法務省における重要な施策を確実に遂行するため、「平成28年度法務省対策推進計画」に基づき、①法務省全体のリスク評価の実施とセキュリティ対策の総合的な強化に向けた行動計画の策定、②情報セキュリティ体制全体の最適化及び③情報セキュリティポリシー等の抜本的な見直し等を行うことにより、情報セキュリティインシデントに迅速に対応できる体制の充実を図ることとしている。

### (1) 体制の整備についての方針

政府全体として、セキュリティ・ITに係る統括部局及び社会的な影響の大きいシステムを所管する部局について、体制の整備を図ることとされていることから、法務省においては、上記対策を強力に推進していくため、平成29年度は、サイバーセキュリティ対策強化の確実な実施及び複数部局が連携し運用する社会的な影響の大きいシステムの安定稼働の確保を重視し、体制の整備を図ることとする。

また、統括部局においては、高度専門人材に当たる民間専門業者とアドバイザー契約を結ぶなどして、セキュリティ・ITに係る助言等が常時受けられる体制の導入を検討することとする。

### (2) 人材の拡充についての方針

法務省においては、国民の取引の安全と円滑に資する登記制度に関する業務、国家社会の治安維持を目的とする捜査・公判・刑の執行等に関する検察業務、矯正施設における被収容者の処遇に関する業務、更生保護に関する業務、出入国管理業務及び破壊的団体の規制に関する調査・処分請求等の業務等を所管しているところ、各組織の所掌業務がそれぞれ高度の専門性・特殊性等を有していることから、それら所掌業務を担う職員の採用・人事管理は各組織ごとに行っている。各組織が保有する情報システムの規模、取り扱う情報の性質、機微度等も様々であり、セキュリティ・IT人材に関しても、研修・教育を通じて一定の育成を行ってはいるものの、総じて有為な人材の確保及び中長期的な計画に基づく育成が必ずしも十分になされているとは言い難い状況にある。

今後のセキュリティ・IT人材の確保・育成についても、基本的には、各組織ごとの人事管理の方針に基づき行うこととなるが、総合強化方針の趣旨を踏まえ

た上で、今後は、下記2ないし5により、計画的にセキュリティ・IT人材を拡充させていくこととする。

また、育成に当たって、各組織において「橋渡し人材」の候補として選考したセキュリティ・IT人材について、セキュリティ・ITに係る統括部局である大臣官房秘書課情報管理室への配置を積極的に検討することで、計画的に育成していくこととする。

## 2 有為な人材の確保

職員を採用する際に、各組織の必要性に応じて、採用者を「橋渡し人材」の候補として育成していくことを視野に入れる場合は、面接において、選定要素の一つとして、セキュリティ・ITに関する知識、資格及び経験の有無、セキュリティ・IT関係業務への意向等についても、確認することとする。

民間企業等においてセキュリティ・IT関係業務に従事した経験のある者を「橋渡し人材」の候補として採用する場合は、経験したセキュリティ・IT関係業務の内容や資格等を確認するとともに、法務省における一般行政事務への意向等についても確認し、採用後は、一般行政事務についての育成も併せて行うものとする。

各組織の必要性に応じて、在職中の職員についても、セキュリティ・IT関係業務への意向等を確認し、その能力、適性等を踏まえた上で、「橋渡し人材」の候補となり得る職員を選考することとする。

## 3 法務省におけるセキュリティ・IT人材育成支援プログラム

法務省では、セキュリティ・ITに関する一定の専門性が必要となる「橋渡し人材」の育成を図るため、「橋渡し人材」の候補となり得る職員について、下記4に記載するセキュリティ・ITに関する部署におけるキャリアパスを念頭に置いて、内閣官房及び総務省において実施するレベル別の研修を受講させるとともに、関係機関と必要な調整を行った上で、インシデント対応等に係る業務を経験させるために内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）へ、情報システムに係るプロジェクト推進及び管理に関する業務を経験させるために内閣官房情報通信技術総合戦略室（以下「IT総合戦略室」という。）へ出向させ、必要に応じその他政府部内機関へも出向させることとする。

## 4 人事ルート例（キャリアパスのイメージ）

「橋渡し人材」は、セキュリティ・ITに関する一定の専門性のみならず、高度専門人材と一般行政部門との橋渡しをするために、法務行政に関する十分な知識・経験を有する必要があるため、その育成に当たっては、セキュリティ・ITに関係する部署における業務経験（キャリアパス）のみならず、法務行政を担う各組織・部署における業務を各役職段階別に経験させるなど、法務行政全般に関する十分な経験、知識、能力の習得を図ることとする。



セキュリティ・ITに関係する部署におけるキャリアパスの一例は以下のとおりである。

(1) キャリアパス像

ア 採用・係員クラス

- ・ 研修： レベルA及びレベルBの研修
- ・ 配属： 大臣官房秘書課情報管理室又は各局部課等における情報システム関連部署の係員
- ・ 出向： NISC又はIT総合戦略室等

イ 係長クラス

- ・ 研修： レベルC以上の研修
- ・ 配属： 大臣官房秘書課情報管理室又は各局部課等における情報システム関連部署の係長
- ・ 出向： NISC又はIT総合戦略室等

ウ 課長補佐クラス

- ・ 研修： NISC及び総務省において新設される実践的な演習等の研修
- ・ 配属： 大臣官房秘書課情報管理室又は各局部課等における情報システム関連部署の室長補佐又は課長補佐
- ・ 出向： NISC又はIT総合戦略室等

エ 管理職

- ・ 研修： NISC及び総務省において新設される実践的な演習等の研修
- ・ 配属： 大臣官房秘書課情報管理室又は各局部課等における情報システム関連部署の室長又は課長

オ サイバーセキュリティ・情報化審議官等

- ・ 研修： サイバーセキュリティ・情報化審議官等研修

(2) キャリアパスの省内配属先として、セキュリティ・ITについて経験することが想定される部署及び役職の一例

ア 大臣官房秘書課情報管理室

- ・ 室長
- ・ 室長補佐
- ・ 法務専門職
- ・ 係長
- ・ 技術専門職

イ 民事局総務課登記情報センター室

- ・ 室長
- ・ 室長補佐
- ・ 法務専門職
- ・ 係長

- ウ 矯正局総務課情報システム管理係
  - ・ 課長補佐
  - ・ 法務専門職
  - ・ 係長
- エ 保護局総務課
  - ・ 課長
  - ・ 法務専門職（企画調整官）  
（情報システム管理係）
  - ・ 課長補佐
  - ・ 法務専門職
  - ・ 係長
- オ 入国管理局出入国管理情報官
  - ・ 出入国管理情報官
  - ・ 情報官補佐
  - ・ 法務専門職
  - ・ 係長
- カ 最高検察庁総務部情報システム管理室
  - ・ 室長
  - ・ 室長補佐
  - ・ 係長
- キ 公安調査庁総務部総務課
  - ・ 上席公安調査専門職
  - ・ 課長補佐
  - ・ 公安調査専門職
  - ・ 上席調査官

## 5 一般行政職員の情報リテラシー向上

セキュリティインシデントの発生を未然に防ぎ、また、発生したセキュリティインシデントに迅速かつ確実に対応する等、組織全体のセキュリティ能力向上のためには、セキュリティ体制の整備、セキュリティ対策の実施やセキュリティ・IT人材の確保・育成だけでなく、一般行政職員の情報リテラシー向上による底上げも必要不可欠である。

法務省では、セキュリティ・ITに関する一般行政職員のリテラシー向上のために、従前からセキュリティ教育等を実施してきたところであるが、今年度以降はPDCAサイクルにのっとり、セキュリティ教育の内容や実施方法の見直し、評価及び改善を行うなどして、有効なセキュリティ教育を実施するとともに、一般行政職員に次の研修を積極的に受講させることとする。

### (1) 全職員向け研修

- ・ 研修名 : 情報システム統一研修（総務省行政管理局）
- ・ 受講対象者 : 一般行政職員
- ・ 受講予定者数 : 1, 800名程度（平成29年度目標。延べ人数）
- ・ 実施時期 : 通年
- ・ 実施方法 : eラーニング及び集合研修

また、上記研修のほか、サイバーセキュリティ月間に合わせて、法務本省内に所属する一般行政職員を対象とした情報セキュリティ研修（集合研修）を実施することとし、一般行政職員100名以上の受講を目標とする。

## (2) その他の各種研修等

各研修実施機関において実施している新規採用職員向け研修、管理職等の各役職段階別研修、選抜・登用研修等の各種研修において、当該研修受講者に応じて求められるセキュリティ・ITに関するリテラシー向上のための講義、eラーニング等を実施する。

また、各庁等の各職場単位においても、必要性に応じて、セキュリティ・ITに関するリテラシー向上のための職員向け研修等を実施する。

## (3) 研修教材等の提供

大臣官房秘書課情報管理室は、必要性に応じて、各研修実施機関、本省局部課、所管各庁等に対し、法務省独自に実施した研修又は内閣官房及び総務省等が実施した研修における教材並びにセキュリティ・ITに関する各種参考資料等を随時送付する。

# 外務省情報セキュリティ・IT人材確保・育成計画

## [概要版]

平成28年8月31日

外務省

### はじめに

#### (1) 経緯

外務省では、国民の生命と財産を守り、外交機密という重要情報を取り扱うとの認識のもと、それらの業務を支える各種システムの運用・管理を担う情報セキュリティ・IT人材の確保と育成を行ってきた。また、全世界に200以上の在外公館が設置されており、環境や公館の規模に応じて、外交や邦人保護を含む領事業務等に関わる社会的影響の大きなシステムを含め、それに適したシステムの構築や運用体制の整備を行っているという特殊性がある。従来から、情報セキュリティ及び情報システム従事者は、総務省が体系的に提供している情報システム統一研修の活用や、当省独自の取組として行ってきた外部研修受講により一定レベルの技術スキルを習得してきたが、情報通信部門や大規模システム保有課室以外でシステムの運用管理を行っている担当者等も含め、当省においてITに携わる全ての関係者が必ずしも情報セキュリティやITに精通しているとはいえない。

今後、情報システムはより多様化・複雑化することが想定されるが、技術的知見をもつ職員の人数不足に加え、プログラミング等のシステム開発そのものに従事した世代の職員が高齢化し、この先10年以内には定年による大量退職時期を迎えるなど、情報セキュリティ・IT人材の不足はますます深刻となる状況であり、技術的人材の育成・確保は急務である。さらに、サイバー攻撃は、地理的な制約を受けることが少なく容易に国境を越えるという特性があるところ、数多くの二国間・多国間協力の枠組みを通じた「サイバー外交」の推進という我が国外交政策上の重要性も益々高まっており、技術的知見をもつ人材だけではなく、技術・政策の両面の知見をもつ職員の育成も課題となっている。

については、政府全体として「サイバーセキュリティ人材育成総合強化方針（平成28年3月31日サイバーセキュリティ戦略本部決定）」が示されたこともあり、これまでの実施施策を踏まえ、外務省として「情報セキュリティ・IT人材確保・育成計画」を新たに策定することとした。

## (2) 目的

本計画は、外務省で所管する情報システムが、外交を支えるインフラとして重要なシステムであることを踏まえ、引き続き、情報システムの適切な運用管理とサイバーセキュリティ対策強化のため、CSIRT（GISIRT）およびSOCとも連携し、省全体として情報セキュリティ及びIT人材の育成・確保を図ることを目的に、以下のとおり平成29年度から平成32年度までの4年間を対象として「外務省情報セキュリティ・IT人材確保・育成計画」として策定したものである。

省内が一体となって本計画の着実な実施に向けて取り組むものとし、情報セキュリティ・IT人材の確保・育成状況等を踏まえ、毎年度末に実施計画の結果を評価し、PDCAサイクルに基づき、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

### 1 体制の整備と人材の拡充

外務省では、情報セキュリティ・ITに係る統括部局の体制の整備及び外交を支えるインフラとして重要なシステムを所管する部局の体制整備として、情報セキュリティ・情報システム・情報ネットワークの3分野を担う人材の確保・育成を重視し、必要な定員要求を行う。また、人材の拡充及び能力の向上のために、今後4年間においても継続して省内システムを有する部門での管理運用業務の経験、他府省への職員の出向等を通じて、育成人材に対する情報セキュリティ及びITに関する研修の実施等を行う。なお、省内の情報セキュリティ対策と情報システム管理並びにこれと一体となった業務改革を、統一性・統合性を確保しつつ一層推進する組織として平成28年3月に設置した情報セキュリティ・情報化推進タスクフォースの強化策を検討する。

### 2 有為な人材の確保

毎年度、技術系一般職を2名程度新卒採用することや技術系総合職相当の職種についても採用の必要性を継続的に検討していく。その際、採用時の面接等で情報セキュリティやITに係る素養及び関係業務への意向を確認することとする。新卒採用により確保した人材については、OJT、出向、研修等を通じて情報セキュリティ・ITに関する能力等の育成、適性の評価等を行うものとする。また、当初から技術系として採用した職員のみならず、他の一般職員についても、本人の意思・適性や当省における人材需要

等を勘案しつつ、情報セキュリティやIT分野の専門家として育成し、主として当該分野で活躍させることも引き続き実施していく。

「橋渡し人材」（セキュリティ・ITに関する一定の専門性と、所管行政に関する十分な知識・経験を有し、高度専門人材（セキュリティ・ITに関する高度な専門性を有する民間等の人材）と一般行政部門との橋渡しをする人材）については、既存の担当者及び新卒採用者からの育成を基本としつつ、業務や組織マネジメントにも通じた情報セキュリティ・ITに関する専門人材の早期確保が必要であることから、民間企業等における情報セキュリティ・IT関係業務に携わった経験のある者を必要に応じて中途採用するなどして、省内での人材育成を補完する。なお、中途採用に当たっては、情報セキュリティ・IT関係業務への意向及びこれまでに経験した業務内容や資格等を確認することとする。また、中途採用により確保した人材については、情報セキュリティ・IT関係の能力の向上に加え、省内における実務を通じた一般行政事務についての育成も併せて行うものとする。

### **3 情報セキュリティ・IT人材育成支援プログラム**

外務省では、以下の点を重点的に取り組むことにする。

- » PMO（Program Management Office：省内のIT施策に関する全体管理の機能を担う組織）、PJMO（Project Management Office：プロジェクトを遂行し、その進捗等を管理する機能を担う組織）に従事する者には、総務省情報システム統一研修（プロジェクト管理）を受講させ、そこで得た知識をベースとして、更にOJTにより必要スキルを習得させる。
- » 橋渡し人材のための情報セキュリティ及びITに関する研修としては、eラーニング及び集合研修を活用し、毎年25名程度の受講を目標とする。また、情報セキュリティについては国家安全保障局及び内閣サイバーセキュリティセンター、情報システムについてはIT総合戦略室及び総務省行政管理局、マイナンバー及び個人情報については個人情報保護委員会事務局に、それぞれ出向することを目途に関係機関との調整等を行うことを検討する。

また、研修によって得られた成果については、省内業務での実務及び資格の取得推進等により、情報セキュリティ・ITに関する能力向上を継続してフォローしていく。

## 4 人事ルート例（キャリアパスの一例）

### （1）全体的なキャリアパス像

外務省では、情報システムの適切な運用管理とサイバーセキュリティ対策強化やサイバー外交政策立案能力強化のため、必要な知識、経験を有する職員を確保・育成していくこととしている。技術系一般職及び一般職（情報セキュリティやIT分野の専門家として育成する人材）のキャリアパスの一例は次のとおりである。なお、技術系総合職相当の職種のキャリアパスについては、本人の意思・適性或当省における人材需要等を勘案しつつ、安全保障政策課企画官、情報通信課長、サイバーセキュリティ・情報化参事官、サイバー政策担当大使等への配置が想定される。

#### ◆係員級（新卒採用を含む）

- ・研修：情報セキュリティ、情報システム、プロジェクト・マネジメントの基礎的な内容に関すること
- ・所属部署：大臣官房情報通信課(企画系班、技術系班、運用系班)、在外公館(通信担当官)勤務
- ・出向等：国家安全保障局、内閣サイバーセキュリティセンター、民間企業など

#### ◆係長級（技術系一般職及び一般職で相当年数後の選考による）

- ・研修：情報セキュリティ、情報システム、プロジェクト・マネジメントおよびインシデント対応の実践・応用的な内容に関すること
- ・所属部署：大臣官房情報通信課（企画系班、技術系班、運用系班）、省内システム保有課室、在外公館(大規模主要公館の広域担当官サブ)勤務
- ・出向等：国家安全保障局、内閣サイバーセキュリティセンター、民間企業など

#### ◆課長補佐級（技術系一般職及び一般職で相当年数後の選考による）

- ・研修：マネジメント研修、インシデント対応に関すること。主に管理職としての判断、指示に関わること

・所属部署：大臣官房情報通信課（企画系班，技術系班，運用系班），省内システム保有課室，在外公館（大規模主要公館の広域担当官）勤務

・出向等：国家安全保障局，IT総合戦略室，総務省行政管理局，民間企業など

◆管理職（技術系一般職及び一般職で相当年数後の選考による）

・研修：マネジメント研修，インシデント対応に関すること。主に管理職としての判断，指示に関わること

・所属部署：大臣官房情報通信課

・出向等：国家安全保障局，内閣サイバーセキュリティセンター，IT総合戦略室

**（２）キャリアパスに含めることが想定される部署**

外務省において，情報システムやサイバーセキュリティ対策に関係する部署として技術系一般職及び一般職（情報セキュリティやIT分野の専門家として育成する人材）職員の配属が想定される部署は次のとおりである。

① 情報セキュリティについて経験することが想定される課室

- i) 大臣官房情報通信課
- ii) 大臣官房IT広報室（統合Web環境所管）
- iii) 領事局政策課（領事業務情報システム所管）

② 情報システムについて経験することが想定される課室

- i) 大臣官房人事課
- ii) 大臣官房情報通信課
- iii) 大臣官房会計課
- iv) 大臣官房在外公館課
- v) 大臣官房IT広報室（統合Web環境所管）
- vi) 領事局政策課（領事業務情報システム所管）

③ 事案対処，情報管理，危機管理，サイバー外交政策等について経験することが想定される課室



- i) 大臣官房総務課情報防護対策室
- ii) 大臣官房総務課外交記録・情報公開室
- iii) 大臣官房情報通信課
- iv) 総合外交政策局安全保障政策課

- ④ 一般行政事務について特に経験をさせたい部署の業務及び想定される課室  
省内各課室の一般行政事務，在外公館の官房・領事・広報業務

## 5 全職員の情報リテラシー向上

外務省では、情報セキュリティ及びシステム利用に関する全職員のリテラシー向上のため、次の研修を実施することとしている。なお、関連研修の受講や資格の取得については業績評価の対象として含め、職員の意欲を高めるようにしている。

必要に応じ総務省情報システム統一研修のeラーニングで提供される研修（情報システム入門，情報セキュリティ基礎等）の受講により意識向上を図る。

### ○全職員向け研修

- ・研修内容：情報セキュリティ研修，標的型メール等への理解
- ・受講対象者：全職員
- ・受講予定者数：全職員（希望者）
- ・実施時期：適宜（年1～2回）
- ・実施方法：eラーニング，標的型メール訓練等

### ○新規採用職員（中途採用含む）及び外務省以外への出向者向け研修

- ・研修内容：情報セキュリティ基礎及びITリテラシー
- ・受講対象者：新規採用職員
- ・受講予定者数：新規採用者数
- ・実施時期：毎年春および秋
- ・実施方法：eラーニング，外部有識者による講義形式等

### ○役職段階別省内研修

- ・研修内容：情報セキュリティ演習
- ・受講対象者：GISIRT, サイバー担当者, システム担当者
- ・受講予定者数：毎年60名程度
- ・実施時期：毎年1～2回
- ・実施方法：外部有識者を招いた講義及び演習（ワークショップ）形式

○省内一般職員向け啓発セミナー

- ・研修内容：情報セキュリティに関する啓発, 業務上の注意事項等
- ・受講対象者：省内一般職員
- ・受講予定者数：毎年50名程度
- ・実施時期：適宜
- ・実施方法：外部有識者またはCISO補佐官による講義形式

○在外公館の通信担当者向け研修

- ・研修内容：情報セキュリティ啓発, 通信業務における注意事項等
- ・受講対象者：在外赴任予定者
- ・受講予定者数：毎年100名程度
- ・実施時期：適宜（毎月1回程度）
- ・実施方法：大臣官房情報通信課担当者による講義形式

○在外公館現地職員向け研修

- ・研修内容：情報セキュリティ啓発, 業務上の注意点等
- ・受講対象者：在外公館で勤務する現地職員
- ・受講予定者数：在外公館で勤務する現地職員
- ・実施時期：適宜（年1回程度）
- ・実施方法：eラーニング, 標的型メール訓練等

以上

平成 28 年 8 月 31 日  
財務省情報化統括責任者（CIO）  
財務省最高情報セキュリティ責任者（CISO）

## 財務省セキュリティ・IT 人材確保・育成計画【概要版】

### はじめに

本計画は、政府全体の世界最先端 IT 国家の実現に向けた取り組み等を踏まえ、財務省が所管行政遂行のためのシステム整備・活用之际し、脅威の高まりが指摘されている環境下でサイバーセキュリティ対策を確保しつつ、業務改革・行政効率化を進めていくための人材確保・育成を目的として策定するものである。

財務省のシステムの運営は、予算編成、税務執行、税関行政等、所管行政に関する基本的な知識・経験を有する職員を中心に担われていることから、従来から職員研修を実施し情報セキュリティの確保等に取り組み、また、インターネット接続については個人情報保護の観点も踏まえ全省的にセキュリティ対策を講じてきたところである。

他方で、セキュリティ対策の適切な高度化を図り、効率的な行政運営の実現に一層努めていくためには、今後、職責・必要性に応じたきめ細かな研修受講、最新の状況を踏まえたセキュリティ意識の向上が課題であると考えられる。また、セキュリティ対策及び適切な調達を全省的に実現するため、部局横断的な情報共有の強化、最新情報を踏まえた調達等にも取り組む必要がある。なお、出向等を通じた人材育成については、受入先と派遣元との適切な要望の調和が課題であると考えられる。

これらの課題に対処するため、部局間のシステムに関するノウハウ等を全省的に共有し最適化を推進する観点から、各部局の実情を踏まえ、橋渡し人材を育成していくと共に、調整する統括部局の強化を図ることとする。本計画は、平成 31 年度までの 4 年間の計画として策定し、必要に応じて適切かつ柔軟に見直しを行っていくこととする。

### 1. 体制の整備と人材の拡充

財務省においてはサイバーセキュリティ対策に係る司令塔機能強化のため、平成 28 年度にサイバーセキュリティ・情報化審議官を設置したが、統括部局においては、今後、

①最新のセキュリティ情勢等を踏まえた部局横断的な情報共有の強化

②各部局のシステム更改等の機会をとらえた、セキュリティ対策強化のための情報共有・調整

③職位・階層に応じた情報発信、研修の企画・調整の充実

④組織横断的な PDCA サイクルの確立・充実

の観点から体制の充実を図るとともに、

⑤「国の行政の業務改革に関する取組方針」（平成 28 年 8 月 2 日総務大臣決定）や「霞が関の働き方改革を加速するための重要取組方針」（平成 28 年 7 月 29 日内閣官房内閣人事局決定）等も踏まえ、財務省内の業務改革を、IT を活用しつつ推進していくため、所要の機構・定員要求を行うこととする。

システム所管部局においても、最新の政府統一基準やガイドライン等を踏まえたシステム設計及びその運用を適切に行う観点から、部局の実情に応じて必要な機構・定員要求を行うこととする。

財務省所管システムの運営は、所管行政に関する基本的な知識・経験を有する職員を中心に担われており、担当職員についてはセキュリティ対策に関する知識等の習得・高度化などを、職務内容・職位に応じ、習得させる必要がある。このような観点から、職員の任用等の時期も勘案しつつ、付加的な研修の充実を計画的に図っていく（下記 3.）。

また、統括部局での勤務や出向等を通じ、専門性を深め、横断的な視野の涵養等も図ることとする。

なお、財務省では、高度の専門性を備えた外部人材の登用や CIO 補佐官による IT 化・セキュリティ対策の充実にも努めており、今後も、先端的な情報・高度の専門性などは外部専門家による補完を適切に講じていく。

## 2. 有為な人材の確保

橋渡し人材候補として育成していくことを視野に入れた人材を確保するため、採用時の面接等において情報セキュリティや IT に係る素養及び関係業務への意向を確認するなど、橋渡し人材候補者となり得る職員の確保に努めることとする。ただし、橋渡し人材については「所管行政に関する十分な知識・経験」を要することや、職員のモチベーション維持の観点からも、セキュリティや IT に係る業務以外にも、多様な勤務経験を積ませることを前提とする。

橋渡し人材候補者は、採用後の身上把握等において「セキュリティ・IT 関係業務」に対する希望の確認や適性を有すると判断された職員の中から、セキュリティ・IT 関係業務部門における OJT、関係機関への出向や必要な研修の受講等を通じてセキュリティ・IT 関係の能力等を育成するとともに、適正性の有無の判断等を行う。なお、所管システムに関しては定期的な更新が計画的に行わ

れることから、セキュリティ対策を含むシステム関連業務の専門性を備えた人材は、ワーク・ライフバランスの観点からの展望を持つことが相対的に容易になることも考えられ、当該分野を希望する誘因となりうる。このように、システムの運営に関わる業務については、計画的な働き方が期待できる分野でもあり、ワーク・ライフバランスが求められる育児や介護等時間制約のある職員も含めて、その人材の確保・育成を検討するものとする。

また、橋渡し人材については、部内での育成を基本としつつ、民間企業等における情報セキュリティ・IT 関係業務に携わった経験のある者を必要に応じて採用等していく。なお、採用等に当たっては、これまでに経験した業務内容や資格等を確認することとする。

### 3. セキュリティ・IT 人材育成支援プログラム

総務省の情報システム統一研修等の外部研修については、職員の任用等の時期も勘案しつつ、受講を計画的に推進する。

また、財務省内で個別のシステム等に対応して実施されている研修の機会をとらえ、統括部局が関与することにより、直近のインシデント事例等最新の状況を踏まえたセキュリティ対策の内容を充実させる。

OJT については、職員の適性等も見極めつつ、統括部局での勤務経験等を通じて、各部局の業務や個別のシステムの知識等に加え、セキュリティに関する意識の向上、横断的な視野の涵養を図る。

従来から実施している NISC、IT 室、総務省行政管理局等への出向についても、同様の観点から活用するが、その際、職員に必要な情報セキュリティスキル・IT スキルが取得できるポストへの出向等の派遣元としての要望と受入先の要望との適切な調和を図るべく調整する。

### 4. 人事ルート例（キャリアパスのイメージ）

#### (1) 全体的なキャリアパス像

財務省では、情報システムの適切な運用管理とサイバーセキュリティ対策を指揮監督する体制を整備するとともに、セキュリティ・IT 人材（橋渡し人材）として「セキュリティ・IT に関する一定の専門性と所管行政に必要な知識、経験を有し、高度専門人材と一般行政部門との橋渡しをする人材」を確保・育成することとしている。こうした情報システムやサイバーセキュリティ対策に関係する経験や知識・能力の習得に加え、所管行政に必要な知識、経験も付与するといった観点を踏まえ、財務省採用後に想定されるキャリアパスの例を示せば、次のとおりである。

- ◆ 採用・係員
  - ・ 研修：情報システム統一研修（A～B レベル）
  - ・ 配属：地方支分部局 ⇒ 財務省及び国税庁（統括部局、システム所管部局、一般行政部局）
  
- ◆ 係長クラス（10年目頃）
  - ・ 研修：情報システム統一研修（C～D レベル）
  - ・ 配属：財務省及び国税庁（統括部局、システム所管部局、一般行政部局）、他府省等への出向
  
- ◆ 課長補佐クラス（20年目頃）
  - ・ 研修：情報システム統一研修（C～D レベル）
  - ・ 配属：財務省及び国税庁（統括部局、システム所管部局、一般行政部局）、他府省等への出向
  
- ◆ 管理職以上（個別）
  - ・ 配属：財務省及び国税庁（統括部局、システム所管部局、一般行政部局）、他府省等への出向等

(2) キャリアパスに含めることが想定される部署

情報システムやサイバーセキュリティ対策、業務改革に係る部署として職員の配属が想定される部署は、統括部局及びシステム所管部局である。

**5. 一般職員の情報リテラシー向上**

情報システム及びセキュリティに関する一般行政職員のリテラシー向上のため、全職員を対象とした研修及び訓練を引き続き実施していく。

こうした従来の取組に加え、サイバー攻撃やインシデント発生等の最新の状況を踏まえ、各種会議の機会等も活用し、訴求対象に応じた情報発信を強化することにより組織のセキュリティ対策水準の向上を図る。

具体的な研修等の実施については、以下のとおり予定している。

- ・ 省内全職員向け研修
- ・ 省内全職員向け訓練
- ・ 省内幹部向け説明
- ・ 地方支分部局幹部級への説明

- ・ システムを所管する省内部局・独法等所管部局・会計担当部局等への説明会
- ・ 外部講師等による勉強会
- ・ 省内新規転任者向け研修
- ・ 地方支分部局における研修
- ・ 地方支分部局における訓練

# 文部科学省サイバーセキュリティ・IT人材確保・育成計画概要版

平成28年8月29日

行政情報化推進委員会／情報セキュリティ対策委員会決定

## はじめに

文部科学省においては、日々、高度化・巧妙化するサイバー攻撃等への対応や業務の効率化を推進する情報化推進業務に対応すべく、大臣官房政策課情報システム企画室を統括部局とし、情報システムを保有する部局に加え、国立大学法人や独立行政法人等の関係機関における所管部局と連携し、関連する研修や訓練の実施を強化するとともに、関係機関との人事交流等を通じた即戦力の確保や育成を行ってきた。

しかしながら、その後もサイバーセキュリティに対する脅威は増大する中で、平成27年5月には日本年金機構によるサイバー攻撃に伴う情報流出事案が発生する等、現状の体制の中で対応していくには限界に達してきている状況にある。

このような情勢の中で、政府全体としても、平成28年3月31日にサイバーセキュリティ戦略本部にて「サイバーセキュリティ人材育成総合強化方針」を決定したが、この中で「セキュリティ・IT人材確保・育成計画（仮称）」を各府省庁にて作成することが掲げられた。

文部科学省においては、所管する情報システムが各部局横断的に存在していることや、今後の霞ヶ関の働き方改革や業務改善（BPR）も視野に入れつつ、「世界最先端IT国家創造宣言」（平成25年6月14日閣議決定 最終改訂平成28年5月20日）の主旨を踏まえ、これまで以上に統括部局と情報システムを保有する部局や関係機関を所管する部局が緊密に連携し、サイバーセキュリティ対策や情報化を一層推進するため、平成31年度までを計画期間として、既存組織の体制強化とその体制を担う人材の確保・育成を目指した「文部科学省サイバーセキュリティ・IT人材確保・育成計画」を以下のとおり策定する。

文部科学省では、本計画の着実な実施に向けて取り組むものとし、サイバーセキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

## 1. 体制の整備と人材の拡充

現在、文部科学省においては、大臣官房政策課情報システム企画室がPMO（Program Management Office）の実務を担当する部局として、社会的な影響の大きいシステムをはじめとする各種情報システムを所管する部局であるPJMO（Project Management Office）に対し、情報システムの構築・運用時に必要な助言等を行う体制を構築しているが、この枠組みが、特にPJMOに十分理解されているとは言えないことから、対応が後手に回る



ことが多く、ときにはPMOへの過度な負担となることもある。この状況を解消するため、本計画策定を機に、改めてPJMOに対して役割と実施すべき事項の理解を促す。

以上を踏まえ、文部科学省では、サイバーセキュリティ・ITに係る統括部局及び社会的に影響の大きいシステムを所管する部局の体制整備として職員のスキル向上を重視し必要な措置を図る。また、サイバーセキュリティ・IT人材の拡充及び能力の向上のために、他省庁や関係機関への職員の出向、サイバーセキュリティ・ITに関する研修の実施を行う。

## **2. 有為な人材の確保**

文部科学省では、本計画期間中に、職員を新規採用するほか、文部科学省関係機関等からも、サイバーセキュリティ・IT関係業務経験を有する者を必要に応じて中途採用し、橋渡し人材候補として育成していくことを視野に入れた人材を確保する。なお、採用に当たっては、サイバーセキュリティ・ITに係る素養等を確認することとする。

## **3. セキュリティ・IT人材育成支援プログラム**

文部科学省では、サイバーセキュリティ・ITに関する研修については、総務省情報システム統一研修やNISC等が実施する橋渡し人材を育成するための研修を活用し、毎年80名程度の受講を目標とする。また、文部科学省内においても、サイバーセキュリティ・ITに関する研修を企画し、集合研修やオンライン研修を活用することでより多くの職員に受講の機会を与える。

また、出向等については、橋渡し人材の育成を目的として必要な人数をNISCや個人情報保護委員会事務局に派遣すべく、関係機関との調整等を行うものとする。さらに、研修によって得られた成果は、サイバーセキュリティ・ITに係る統括部局や社会的な影響の大きいシステムを所管する部局等への配属により、サイバーセキュリティ・ITに関する能力やスキルについてフォローを行っていく。

なお、研修等を行うに当たっては、文部科学省関係機関のセキュリティインシデントの急激な増に対応できることや、情報システムの企画立案から管理運用に至る過程に触れる機会を設けるよう努める。

## **4. 人事ルート例（キャリアパスのイメージ）**

文部科学省では、情報システムの適切な運用管理とサイバーセキュリティ対策の指揮監督体制を整備し、必要な知識、経験を有する職員を確保・育成していくこととしている。なお、文部科学省採用後に想定されるキャリアパスの一例は次のとおりである。

### **◆採用・係員**

- ・研修：文部科学省において実施する研修  
総務省情報システム統一研修

N I S C主催の勉強会・セミナー

- ・ 出向等：N I S C，個人情報保護委員会事務局

◆係長クラス

- ・ 研修：文部科学省において実施する研修

総務省情報システム統一研修

N I S C主催の勉強会・セミナー

- ・ 出向等：N I S C，個人情報保護委員会事務局

◆課長補佐クラス

- ・ 研修：文部科学省において実施する研修

総務省情報システム統一研修

N I S C主催の勉強会・セミナー

- ・ 出向等：N I S C，個人情報保護委員会事務局

◆管理職

- ・ 研修：文部科学省において実施する研修

総務省情報システム統一研修

N I S C主催の勉強会・セミナー

◆サイバーセキュリティ・政策評価審議官

- ・ 研修：文部科学省において実施する研修

総務省情報システム統一研修

N I S C主催の勉強会・セミナー

総務省及びN I S C主催のサイバーセキュリティ・情報化審議官等研修

## 5. 一般職員の情報リテラシー向上

文部科学省では、情報システム及びサイバーセキュリティに関する一般行政職員のリテラシー向上のため、次の研修を実施することとしている。

### ○オンライン研修

- ・ 研修内容：サイバーセキュリティや行政情報化の最新動向に関する研修
- ・ 受講対象者：全職員
- ・ 受講予定者数：全行政事務従事者（約2,000人）
- ・ 実施時期：年間2回（4月，10月）及び新規にIDを取得した者に対して随時
- ・ 実施方法：eラーニング

### ○新任者向け研修

- ・ 研修内容：新任者として最低限身につけておくべきITの利用に関する研修（レベルA相当）
- ・ 受講対象者：文部科学省情報セキュリティポリシーにおける行政事務従事者として新たに業務に従事する者

- ・ 受講予定者数：毎年300名程度
- ・ 実施時期：4月，10月
- ・ 実施方法：省内職員による講義形式

○一般職員向け啓発セミナー

i) 文部科学省情報セキュリティセミナー

- ・ 研修内容：サイバーセキュリティに関する最新動向等について
- ・ 受講対象者：文部科学省情報セキュリティポリシーにおける行政事務従事者に従事する者（関係機関向けに実施するセミナーの聴講者として募集する予定）
- ・ 受講予定者数：毎年10名程度
- ・ 実施時期：毎年2月頃
- ・ 実施方法：外部有識者を招いた講義形式

平成 28 年度～平成 31 年度  
厚生労働省セキュリティ・IT 人材確保・育成計画書  
概 要

厚生労働省では、「行政機関における IT 人材の育成・確保指針」(H19.4.13 各府省 CIO 連絡会議)に基づいた実行計画を定め人材育成を実施してきたが、本年 1 月に実施した「IT 人材の状況把握に係る実態調査」等により、目標とされたスキルレベルに到達していないことが明らかになった。また、政府全体として「サイバーセキュリティ人材育成総合強化方針」(H28.3.31 サイバーセキュリティ戦略本部)が示されたことから計画を抜本的に見直し、「セキュリティ・IT 人材確保・育成計画」を策定することとした。

### 1. 本計画を策定するに当たっての基本方針

平成 27 年度に発生した日本年金機構における不正アクセスによる情報流出事案を教訓として、情報システム全体を俯瞰して有効かつ効率的なセキュリティ対策を講じていくための厚生労働省内の能力と体制を整える。

戦略的投資としての情報システムを最適化できる IT 人材を育てることにより、政策を企画し遂行し実現する組織能力を高める。

新しい技術の登場により、情報システムが直面するリスクは常に変化していくので、省内、政府内、さらには民間との人事交流等を通じて知識・スキルの代謝が進められるよう、専門領域にとらわれず IT 人材のキャリアパスを設計する。

組織の文化や風土は、職員の意識によって形作られるものなので、高度な知識・スキルを有する人材の育成を図る一方で、組織全体のレベルアップを実現する。

### 2. 本計画の到達目標

本計画は、平成 31 年度までの間に情報システムの適切な企画、設備等の調達、プロジェクト管理、情報システムの運用管理及びサイバーセキュリティ対策を実施する体制を強化し、その体制を担う人材の確保・育成を進めることを大きな目標とする。

この目標を達成するため、平成 28 年度から平成 31 年度までの 4 年間で計画期間として「セキュリティ・IT 人材育成プログラム」を立案し、実行していく。人材育成は、短期に成し遂げられるものではなく時間を要することから、本プログラムが目指す IT 人材のレベルは、過去の実態調査の結果を踏まえ、4 年間という限られた期間内で確実にステップアップしていくことができるように設定する。

### 3. 体制の整備と人材育成研修の見直し

厚生労働省では、情報システムの適切な運用管理とサイバーセキュリティ対策を推進し、これらと一体となった業務改革に取り組む一環として、平成 27 年に最

高情報セキュリティ責任者（CISO）及び情報化統括責任者（CIO）の位置づけを厚生労働審議官に格上げし、この最高責任者が省内全体を指揮監督できるよう、体制強化にも取り組んできている。

人材の拡充に関しては、新規採用者については必要な知識や能力等の素養を有しているかを評価して電気・電子・情報系の試験区分合格者を積極的に採用することとし、任期付職員採用等によって高度な能力を有する即戦力人材の採用を行っていく。

人材育成に関しては、全省庁の職員が身に着けているべき必須スキルを考慮して内容が作られている総務省情報システム統一研修を最大限に活用する。一方、統一研修を受講できない職員に対しては、補完研修を実施する。

また、情報セキュリティ研修を実施したり、NISC等が主催するサイバーセキュリティのケーススタディ等の実践的な演習やCSIRT要員への研修・訓練に参画させたりして、研修参加の機会そのものを広げていく。

#### 4. 「橋渡し人材」の確保

毎年度、一般職又は総合職の新規採用者から、数名を強化方針に示された「橋渡し人材」候補として育成していく。これら候補者は、統一研修や補完研修だけでなく、研究機関・政府機関への出向や官民交流等の機会を与えて、サイバーセキュリティ及び情報システムの企画、設備等の調達、プロジェクトの管理、情報システム運用管理に関する能力の育成を図るとともに、適性を判断していく。

#### 5. セキュリティ・IT人材育成プログラム

職員は、統一研修を可能な限り受講することを人材育成研修の基本とする。この統一研修を有効に利用するためには、受講者がそのレベルに合った研修コースを選択する必要がある、この選択によって個々の研修の効果が高まるようにしていく。情報システムのプロジェクトに携わった経験がない一般職員には、「一般職員のICT活用基礎能力の習得」の中の「情報システム入門」を受講するよう導き、PMO、PJMOの職員は「情報システムのプロジェクトに携わる職員の知識・能力の向上」に関連するコースを情報システム関連業務の経験に応じた優先順位にしたがって受講させる。

統一研修を基軸にしつつも、研修受講者を増やしIT人材のレベルアップを図るため、統一研修のテーマを絞り込んで、期間を短縮して実施する補完研修を行うようにする。

スキルレベルの達成度合いについては、各年度末に評価する。

#### 6. 人事ルート例

情報システムの適切な運用管理とサイバーセキュリティ対策を指揮監督する体制を整備し、必要な知識、経験を有する職員を確保・育成していく観点から、厚生労働省採用後に想定されるキャリアパスの例を設定する。

# 農林水産省セキュリティ・IT人材確保・育成計画（概要版）

平成28年 8月31日

## はじめに

農林水産省は、食料の安定供給の確保、農林水産業の発展、農山漁村及び中山間地域等の振興並びに農林水産関係の国際交渉、国際協力等幅広い政策分野を担当しており、このような特徴に対応して、比較的小規模ながら多種多様な分野にわたる約80の政府情報システムを保有している。

農林水産政策が「攻めの農林水産業」の展開等重要な政策転換期にある中で、農林水産省の情報システムは、農林水産政策の円滑かつ効果的な推進を支える重要な役割を担っている。こうした役割を適切に果たしていくためにも、適時・的確な情報セキュリティ対策を講ずるとともに、情報システムの適切な運用管理を確保することが不可欠である。

平成25年5月に取りまとめられた「農林水産省へのサイバー攻撃に関する調査結果」（以下「調査結果」という。）を真摯に受け止め、情報セキュリティ対策の強化に努めてきたところであるが、複雑化・巧妙化するサイバー攻撃、情報システム改革等に対し適切に対処するため、農林水産省が保有する情報に係るセキュリティの確保及び情報システムの適切な運用管理が一層重要となっている。

このため、最高情報セキュリティ責任者（CISO）・情報化統括責任者（CIO）を補佐する大臣官房サイバーセキュリティ・情報化審議官の主導の下、平成31年度を目途に、情報セキュリティ対策及び情報システムの適切な運用管理を行う体制を整備することとし、その体制を担う人材の確保・育成を図ることを目的に本計画を策定する。

また、本計画の着実な実施に向けて取り組むとともに、情報セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて本計画を見直すものとする。

## 1 体制の整備と人材の拡充

調査結果を踏まえ、平成26年4月に情報セキュリティ対策部署と情報システム管理・運用部署を統合するなどの体制整備を図ってきたところであるが、その後、サイバーセキュリティ基本法の施行、マイナンバー制度の開始、個人情報保護法の改正等、農林水産省が取り扱う情報の重要性が一層高まる中で、それらの情報を適切に管理する体制を整備することが喫緊の課題となっている。

このため、農林水産省における情報セキュリティ・ITに係る統括部署の体制の整備及び社会的に影響の大きいシステムを所管する部署（以下「システム所管部署」という。）の体制整備として、情報システムの活用による更なる業務効率化、個人情報をはじめとするセキュリティの確保等を重視し、必要な機構・定員要求を行う。

また、人材の拡充及び能力の向上のために、平成31年度までの間において、関係府省への職員の出向、一般職員に対する情報セキュリティ等に関する研修を実施し、情報セキュリティ・IT人材の育成に努める。

## 2 セキュリティ・IT人材育成支援プログラム

橋渡し人材の育成に係る研修については、橋渡し人材として必要な知識を習得させる必要があることから、総務省が実施する情報システム統一研修を活用するものとする。

る。具体的には、セキュリティ・ITに係る基礎的な知識及び担当業務に必要な知識を優先して習得することとし、まずは、該当するレベルA、B等のeラーニングを受講し、その後、レベルD1、D2等の集合研修を受講することにより、毎年90名程度（延べ人数）の受講を目途に参加させるものとする。（注）

情報セキュリティ担当者については、これらの研修に加え、内閣官房内閣サイバーセキュリティセンターが実施する勉強会、演習、情報セキュリティ緊急支援チーム（CYMAT）研修といったより実践的な研修を受講するものとする。

また、出向等については、情報セキュリティやITに関する実践的・専門的な業務経験による知見・能力向上につながるものとして、引き続き、内閣官房情報通信技術（IT）総合戦略室、内閣官房内閣サイバーセキュリティセンター、総務省行政管理局及び個人情報保護委員会に派遣することを目途に、関係機関との調整等を行うものとする。

（注：レベル）

A：採用後又は橋渡し人材候補となった後、速やかに受講すべき研修（「電子政府基礎」）

B：係長昇任までに受講すべき研修（「情報システム入門」等ITパスポートレベル相当）

C：係員・係長時に受講すべき研修（「ネットワーク基礎」等基本情報技術者、セキュリティマネジメントレベル相当）

D1：係員・係長時に受講すべき研修（「プロジェクト管理」等応用情報技術者レベル相当）

D2：係員・係長時に受講すべき研修（「IT調達と発注管理」等）

### 3 人事ルート例

#### (1) 全体的なキャリアパス像

橋渡し人材が、情報セキュリティ対策や情報システムに関係する経験や知識・能力を習得する観点から、農林水産省採用後に想定されるキャリアパスの一例は次のとおりである。

##### ◆採用・係員（採用年から6年目頃）

- ・研修：情報システム及び情報セキュリティに関する基礎的な研修
- ・所属部署：統括部署、システム所管部署、統計調査担当部署等

##### ◆係長クラス（7年目頃）

- ・研修：情報システム及び情報セキュリティに関する応用的な研修
- ・所属部署：統括部署、システム所管部署、統計調査担当部署（地方支分部局及び本省）、政策担当部署等
- ・出向：関係府省

##### ◆課長補佐クラス（20年目頃）

- ・所属部署：統括部署、システム所管部署、統計調査担当部署（地方支分部局及び本省）、政策担当部署等
- ・出向：関係府省

##### ◆管理職

- ・所属部署：地方支分部局課長、地方参事官、本省室長、地方支分部局部長、本省課長等

##### ◆サイバーセキュリティ・情報化審議官等

#### (2) キャリアパスに含めることが想定される部署と役職

農林水産省において、情報セキュリティ対策や情報システムに関係する部署として職員の配属が想定される部署・役職等は次のとおりである。

## ア 情報セキュリティについて経験することが想定される部署と役職

- 大臣官房広報評価課情報管理室  
室長、情報セキュリティ、システム整備・管理を担当する情報企画官・課長補佐・係長

## イ 情報システム・業務改革について経験することが想定される部署と役職

- (ア) 大臣官房広報評価課情報管理室（農林水産省行政情報システム及び農林水産省統合ネットワーク）  
室長、システム改革・整備・管理を担当する情報企画官・課長補佐・係長
- (イ) 大臣官房広報評価課広報室（コンテンツ・マネジメント・システム）  
システム担当者
- (ウ) 大臣官房統計部統計企画管理官（農林水産統計システム）  
システムを担当する管理官補佐・係長
- (エ) 食料産業局輸出促進課海外輸入規制対策室（輸出証明書発行システム）  
システム担当者
- (オ) 食料産業局知的財産課種苗審査室（品種登録業務関連システム）  
システム担当者
- (カ) 農村振興局整備部設計課施工企画調整室（農林水産省電子入札システム及び農業農村整備総合支援システム（現場業務支援システム））  
システム担当者
- (キ) 農村振興局整備部水資源課施設保全管理室（農業水利ストック情報データベースシステム）  
システム担当者
- (ク) 農村振興局整備部防災課（国営造成土地改良施設防災情報ネットワーク）  
システム担当者
- (ケ) 政策統括官付総務・経営安定対策参事官付経営安定対策室（経営所得安定対策情報管理システム）  
システム担当者
- (コ) 政策統括官付貿易業務課（政府所有米麦情報管理システム）  
システム担当者
- (サ) 農林水産技術会議事務局筑波産学連携支援センター情報システム課（農林水産省研究ネットワーク、科学技術計算システム及びネットワークサービスシステム）  
システム担当者
- (シ) 横浜植物防疫所リスク分析部（植物防疫所行政情報システム）  
システム担当者
- (ス) 動物医薬品検査所企画連絡室（副作用情報データベース及び動物医薬品等データベース）  
システム担当者
- (セ) 林野庁国有林野部経営企画課（国有林野情報管理システム）  
システム担当者
- (ソ) 水産庁資源管理部管理課（広域資源管理情報処理システム）  
システム担当者



ウ 一般行政事務について、特に経験させたい部署の業務及び想定される課室と役職

- (ア) 大臣官房広報評価課広報室、同課報道室、同課情報分析室  
広報・報道、情報分析を担当する課長補佐・係長
- (イ) 大臣官房統計部の統計調査を担当する課長補佐・係長

#### 4 一般職員の情報リテラシー向上

情報セキュリティ及び情報システムに関する一般職員のリテラシー向上のため、情報セキュリティ対策教育実施計画等に基づき以下の研修を実施する。

また、総務省の情報システム統一研修の中でeラーニングを活用する基礎的な研修（「情報システム入門」等）については、一般職員にとっても必要な知識を習得させるものであり、可能な限り受講させるようにする。

さらに、係長研修、補佐研修、管理職研修等の役職段階別研修においても情報セキュリティ対策等に関する説明を行うことにより、役職に見合ったリテラシー向上を図る。

#### (1) 情報セキュリティに関する研修

##### ア 情報セキュリティに係る一般教育

- (ア) 研修内容：農林水産省における情報セキュリティの組織・体制、情報の格付及び取扱い、情報セキュリティ対策等
- (イ) 受講対象者：全職員
- (ウ) 実施時期：毎年7月
- (エ) 実施方法：eラーニング

##### イ 標的型メール訓練

- (ア) 研修内容：標的型メール攻撃への対応
- (イ) 受講対象者：全職員
- (ウ) 実施時期：毎年9月、12月
- (エ) 実施方法：標的型メールの配信

##### ウ 新規採用者研修

- (ア) 研修内容：農林水産省における情報セキュリティの組織・体制、情報の格付及び取扱い、情報セキュリティ対策等
- (イ) 受講対象者：新規採用者
- (ウ) 受講予定者数：150名程度
- (エ) 実施時期：毎年4月
- (オ) 実施方法：統括部署による講義形式

#### (2) 情報システムに関する研修

##### ○ IT調達事務に係る研修

- (ア) 研修内容：IT調達に係る要件設定、仕様書の作成等について
- (イ) 受講対象者：IT調達事務を担当する者
- (ウ) 受講予定者数：40名程度（延べ人数）
- (エ) 実施時期：毎年4月、10月
- (オ) 実施方法：専門的知識を有する者による講義形式

## はじめに

経済産業省は、情報処理の促進を任務のひとつとしており、自身の電子化にも積極的に取り組んできた歴史を持つ。現在も、基盤情報システムなど経済産業行政の円滑な遂行に不可欠な複数のシステムを運用するとともに、電力・ガスなど社会生活の基盤たる重要インフラの情報セキュリティ対策を始めとするIT政策を遂行している。

これらの取組を円滑に進める上で最も重要なのは、能力と経験を有する人的資源である。このような認識の下、経済産業省では、新規採用等を通じて、省内システムの統括部門、各運用部門、情報政策部門などに一定規模のセキュリティ・IT人材を確保するとともに、本人の希望と能力を踏まえた任用、OJTや省内研修を通じた継続的な人材育成に努めてきた。

他方、近年、サイバー空間が国民生活の一部となるにつれ、行政の円滑な遂行の観点からも、効率的、効果的なシステムの導入、安定運用が一層重要となっている。また、サイバー攻撃が年々激化、巧妙化する中、国民生活に影響を及ぼさぬよう、経済産業省自身や重要インフラ等において常に万全の対策を講じていくことが求められている。

このような課題に対応するため、現在のセキュリティ・IT人材の確保、育成を従来以上に充実させていく必要があり、また、政府全体として「サイバーセキュリティ人材育成総合強化方針」（平成28年3月31日サイバーセキュリティ戦略本部決定）を策定したことも踏まえ、経済産業省における「セキュリティ・IT人材確保・育成計画」を策定することとした。本計画は、経済産業省自身が運営するシステムの安定運用・セキュリティ対策、電力・ガス等の重要インフラを始めとする民間のセキュリティ対策の推進等に関し、これを担う人員の確保、育成を一層強化することを目的とする。

本計画に基づき、後述のとおり、必要な組織体制の強化、採用活動の充実、政府内研修への積極参加などの対策を講じていく。計画期間は、先行的に一部の組織体制を強化した平成28年度から、平成31年度までとする。この4年間の全体方針を示すとともに、特に、直近の平成29年度については具体的な対応策を定める。将来的には、計画の実施状況、サイバー空間を取り巻く状況変化等を踏まえ、必要に応じて柔軟に見直していく。

## 1. 体制の整備と人材の拡充

経済産業省では、昨今の政府関係機関へのサイバー攻撃の増加・高度化に対応するため、セキュリティ対策に係る体制強化を重視し、必要な機構・定員要求を段階的に進めていく。

また、セキュリティ分野に留まらず、広くセキュリティ・ITの専門人材の拡充、能力向上を図る。具体的には、情報分野に関心のある学生向けの採用活動を強化し、入省後は本人の希望や適正を考慮し、省内の専門人材ポストへの配置を行う。総務省のIT統一研修への積

極的な参加、外部機関への出向機会等も活用し、将来的にセキュリティ・IT分野の中枢を担う専門職員の育成を図っていく。

## **2. 有為な人材の確保**

経済産業省は情報処理の促進に関する事務を所掌しており、これまでもITに関する知見を有する人材を採用してきたが、昨今のIT人材の必要性の高まりに鑑み、新卒、中途ともにその採用活動を強化していく。具体的には、情報政策に関する説明会や、情報政策に携わる職員による座談会等を開催し、ITに知見・関心を有する者を確保していくとともに、必要に応じて、毎年数名程度は、将来の情報システム及びサイバーセキュリティ分野における橋渡し人材の候補者として育成していくことを念頭に、一般職、総合職の採用を行っていく。確保した人材については、橋渡し人材候補としての活用を念頭に置きつつ、OJT、出向、研修等を通じて、その能力の向上を図っていく。

## **3. セキュリティ・IT人材育成支援プログラム**

経済産業省では、一定規模のセキュリティ・IT人材に係るポストが存在しているが、それぞれのポストに応じ、セキュリティ対策、プロジェクト管理、システム運用・保守など担当業務は様々であり、当該業務に対応できる能力を身につける必要がある。また、キャリアパスの中でこれらの様々な能力を身につけた職員が「橋渡し人材」となり、高い職責で現場を指揮・指導していくこととなる。

このような問題意識の下、セキュリティ・IT人材に係るポストの職員に対し、内閣官房及び総務省において用意する「橋渡し人材」の候補者向け研修において、そのポストに対応するコースを受講させていく。更に、研修によって得られた成果を業務に生かすべく、任用の際の参考にしていく。

出向等については、これまでも外部機関への出向を多数行っており、今後も継続を見込むとともに、必要に応じて出向先や人数規模に関して見直しを行う。

## **4. 人事ルート例（キャリアパスのイメージ）**

セキュリティ・IT人材に必要な能力は、本人の素質・適正と、経験に裏打ちされた知識の双方が必要である。従って、どのようなキャリアパスを通っていくかというのは重要であり、組織として計画的に育てていくことが必要である。

このため、採用後の係員・係長レベルの若手世代については、幅広い職員に関係部局の経験の機会を与えることが重要と考えている。その中で、本人の適正、希望を見極め、セキュリティ・IT人材の候補と期待される職員には、課長補佐レベルとして一定の責任を持った仕事を経験させる。更に、その中でも優れた能力を発揮する人材については、管理職として現場を指揮・指導していく。

このような考え方をイメージしたキャリアパス例を以下に示す。

◆採用・係員（採用年から5年目頃）

- ・研修：情報システム新任者、情報システム入門 等
- ・所属部署：システム統括部門 等
- ・出向等：内閣官房サイバーセキュリティセンター 等

◆係長クラス（10年目頃）

- ・研修：情報セキュリティ基礎、プロジェクト管理基礎 等
- ・所属部署：情報セキュリティ政策の企画・立案部門 等
- ・出向等：留学 等

◆課長補佐クラス（20年目頃）

- ・研修：情報セキュリティ（技術）、システム運用・保守 等
- ・所属部署：システム運用部門 等
- ・出向等：内閣官房 IT 戦略室 等

◆管理職（25～30年目頃）

- ・研修：情報セキュリティ（管理）、IT 調達と発注管理 等
- ・所属部署：システム統括部門
- ・出向等：内閣官房サイバーセキュリティセンター 等

## 5. 一般職員の情報リテラシー向上

経済産業省では、情報システム及びセキュリティに関する一般行政職員のリテラシー向上のため、次の研修を実施することとしている。

- ① 全職員向け e-learning 研修
- ② 階層別座学研修
- ③ 標的型メール訓練

# 国土交通省セキュリティ・IT人材確保・育成計画 【概要版】

平成 28 年 8 月 31 日  
国土交通省 CIO/CISO 決定

## はじめに

国土交通省は、国土の総合的かつ体系的な利用、開発及び保全、そのための社会資本の総合的な整備、交通政策の推進、観光立国の実現に向けた施策の推進、気象業務の健全な発達並びに海上の安全及び治安の確保など幅広い政策分野を担当しており、これらの業務を遂行する上で、大小様々な約 200 の情報システムを保有・運用している。

これらの情報システムには、その所管部局が多数分散していることに加え、その多くが、多数の個人情報をはじめとする機密性の高い情報を扱う情報システムや、国民の安心・安全を守るために完全性、可用性を求められる情報を扱う情報システムであるという特殊性があり、国土交通省は、こうした特殊性を踏まえつつ、多数の情報システムを自ら運用している。

また、多種多様な独立行政法人（15 法人）や、重要インフラ事業者（鉄道・航空・物流）をはじめとする国民生活に密接に関連する多様な分野を所管しており、これら法人等の情報セキュリティ対策をはじめとする IT 政策を遂行しているところである。

これらの取組を着実に遂行するためには、充実した体制と能力・経験を有する人材が不可欠であり、国土交通省においては、情報システムの整備及び運用に関して、政府共通ルールに基づき、IT ガバナンスの強化に努めているところである。省内のセキュリティ・IT に係る統括部局、各情報システム所管部局等においては、OJT 等を通じた継続的なセキュリティ・IT 人材の育成に努めるとともに、省全体でもサイバーセキュリティに係る研修や標的型メール攻撃訓練等を通じた情報リテラシーの向上を図っている。また、独立行政法人や所管事業者に対しては、セキュリティ・IT に係る統括部局を中心として CISO の任命や CSIRT の設置をはじめとしたセキュリティ体制の構築等を働きかけているところである。

一方、近年では、国土交通省をはじめ、独立行政法人や所管事業者等に対するサイバー攻撃が多数観測・報告されており、その傾向は、2020 東京オリンピック・パラリンピック競技大会に向けて、より一層、高度化・巧妙化・増加することが予想される。

こうした状況において、国民生活に影響を及ぼさぬよう、国土交通省、独立行政法人や所管事業者等の情報システムに係るセキュリティの確保及び情報システムの適切な運用管理がより一層重要となっており、国土交通省自身や所管事業者等において常に万全の対策を講じていくことが求められている。

このため、現在のセキュリティ・IT 人材の確保・育成を従来以上に充実させていく必要があり、また、政府全体として「サイバーセキュリティ人材育成総合強化方針」（平成 28 年 3 月 31 日サイバーセキュリティ戦略本部決定）が策定されたことも踏まえ、セキュリティ・

ITに係る統括部局や社会的影響の大きいシステムを所管する部局に係る体制の更なる整備を図るとともに、これらの部局を担う人材として橋渡し人材の確保・育成を図ることを目的に、以下のとおり平成31年度までを計画期間とする「国土交通省セキュリティ・IT人材確保・育成計画」を策定することとした。

今後、本計画の着実な実施に向けて取り組むものとし、セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

## 1. 体制の整備と人材の拡充

国土交通省では、上記の状況を踏まえ、昨今の政府関係機関や所管事業者へのサイバー攻撃の増加・高度化に対応するため、セキュリティ・ITに係る統括部局や社会的影響の大きいシステムを所管する部局に係る体制整備に重点を置くこととする。

国土交通省では、従来より、CIO補佐官、最高情報セキュリティアドバイザー等も活用しつつ、情報システムに係るセキュリティの確保及び情報システムの適切な運用管理を行ってきたところであるが、それに加え、平成28年4月には大臣官房サイバーセキュリティ・情報化審議官が設置され、一定の体制強化が図られた。

しかしながら、当該審議官の司令塔機能・統括機能を十分に支えるべき統括部局の体制は未だ十分には整備されていないのが現状である。また、情報システム所管部局においても技術の進歩等により今後更に高度化・増加すると予想される業務に対応していく上では、人材の確保・育成や更なる体制の強化が課題となる。このように、セキュリティ・ITに係る統括部局、情報システム所管部局ともに、今後も万全な対策を講じていくための十分な体制と人材が現状において確保されているとは言い難い。

このため、省内において保有・運用している情報システムに係るITガバナンス等の強化や、独立行政法人及び重要インフラ事業者をはじめとする所管事業者に対するセキュリティ対策の推進等を更に図り、情報システムのPDCAサイクルの各段階において、より一層精緻にセキュリティリスクを低減させるため、セキュリティ・ITに係る統括部局の体制の整備を図るとともに、特に社会的に影響の大きいシステムを所管する部局の人材の確保・育成を重視し、橋渡し人材を確保及び育成するために必要な機構・定員要求を行う。

また、人材の拡充及び能力の向上のために今後4年間において、内閣サイバーセキュリティセンター及び個人情報保護委員会への職員の出向、全職員を対象とした情報ネットワーク・セキュリティ研修をはじめ、新規採用職員から役職段階別に情報セキュリティに関する研修の実施等を行う。

## 2. セキュリティ・IT人材育成支援プログラム

国土交通省では、セキュリティ・ITに係る統括部局及び社会的な影響の大きいシステムを所管する部局については、それぞれのポストに応じたセキュリティ対策、プロジェクト管理、システム運用・保守など当該業務に必要な能力を身につけ、幹部職員を含めた全職員に

については、普段からの意識向上を図ることが重要であることから、以下の点を重点的に取り組むこととする。

- セキュリティ・ITに係る統括部局や社会的な影響の大きいシステムを所管する部局に従事する者を対象に、情報セキュリティに関するeラーニングを受講等させるとともに、特にセキュリティ・ITに係る統括部局に従事する者には、総務省統一研修（プロジェクト管理）を受講させるとともに、実業務でのOJTを通じて、必要なスキルを習得させる。
- 上記を含むシステム所管部局等に従事する者を対象に、情報セキュリティ及びITに関する研修については、総務省が実施する「情報システム統一研修」を活用し、毎年200名以上の受講を目処に実施していく。  
また、出向等については、NISC及び個人情報保護委員会に毎年複数名を派遣することを目処に関係機関との調整等を行うものとする。
- 幹部職員を含めた全職員を対象に、標的型メール攻撃訓練や情報セキュリティ対策の自己点検を実施するとともに、情報セキュリティインシデント情報を定期的にとりまとめ省内に周知する等により、意識啓発を図るものとする。

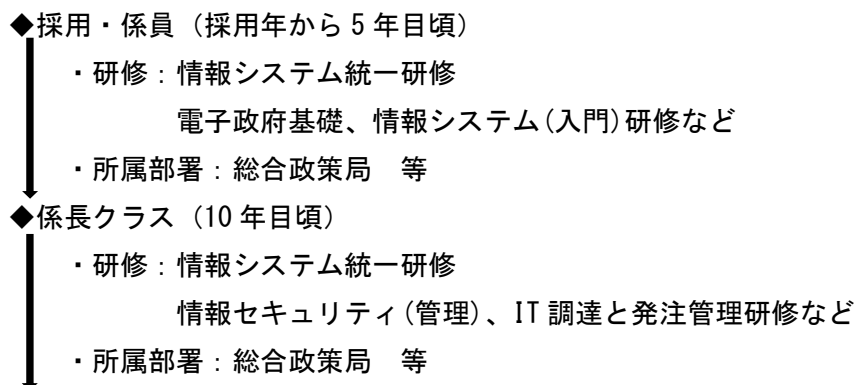
### 3. 人事ルート例（キャリアパスのイメージ）

#### (1) 全体的なキャリアパス像

国土交通省では、情報システムの適切な運用管理とサイバーセキュリティ対策の指揮監督する体制を整備し、必要な知識、経験を有する職員を確保・育成していくこととしている。

こうした情報システムやサイバーセキュリティ対策に関係する経験や知識・能力の習得の観点から、国土交通省採用後に想定されるキャリアパスの一例は次の通りである。

なお、一部部局においては、業務や情報システムの特殊性・専門性を有しており、それぞれにおいて、情報システムの企画・開発に関する技術面・運用面の知識、スキルの継続的な蓄積を図り、継続的な従事を可能とする必要があるため、情報システム関係の専門的知識を持つとともに、現場の運用業務を理解している職員をそれぞれ個別に確保・育成していくこととしている。



- ◆課長補佐クラス（20年目頃）
  - ・研修：情報システム統一研修
  - ・所属部署：総合政策局 等
  - ・出向等： N I S C
- ◆管理職（30年目頃）
  - ・研修：情報システム統一研修
  - ・所属部署：総合政策局 等
- ◆サイバーセキュリティ・情報化審議官等
  - ・研修：情報システム統一研修

(2) キャリアパスに含めることが想定される部署

国土交通省において、情報システムやサイバーセキュリティ対策に係る部署として職員の配属が想定される部署等は次の通りである。

- ① セキュリティについて経験することが想定される課室
  - i) 総合政策局情報政策課
  - ii) 総合政策局行政情報化推進課
  - iii) 国土政策局国土情報課
  - iv) 土地・建設産業局不動産市場整備課
  - v) 自動車局自動車情報課
  - vi) 航空局交通管制企画課管制情報処理システム室
  - vii) 気象庁総務部企画課
- ② 情報システム・業務改革について経験することが想定される課室
  - i) 総合政策局行政情報化推進課
  - ii) 国土政策局国土情報課
  - iii) 土地・建設産業局不動産市場整備課
  - iv) 自動車局自動車情報課
  - iii) 航空局交通管制企画課管制情報処理システム室
  - iv) 気象庁総務部企画課
  - v) 気象庁予報部業務課
- ③ 事案対処、保安、事故対応、危機管理、安全保障等について経験することが想定される課室
  - i) 気象庁総務部企画課
  - ii) 海上保安庁総務部情報通信課

#### 4. 一般職員の情報リテラシー向上

国土交通省では、情報システム及びセキュリティに関する一般行政職員のリテラシー向上のため、次の研修を実施することとしている。



○新規採用職員向け研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：全職員
- ・受講予定者数：毎年 170 名程度
- ・実施時期：4 月
- ・実施方法：講義方式

○役職段階別省内研修

i) 係長研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：全職員
- ・受講予定者数：毎年 220 名程度
- ・実施時期：6 月、7 月、8 月、2 月
- ・実施方法：講義方式

ii) 課長補佐研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：全職員
- ・受講予定者数：毎年 80 名程度
- ・実施時期：6 月
- ・実施方法：講義方式

iii) 課長級研修

- ・研修内容：情報セキュリティ研修
- ・受講対象者：全職員
- ・受講予定者数：毎年 40 名程度
- ・実施時期：1 月
- ・実施方法：講義方式

# 環境省セキュリティ・IT人材確保・育成計画 (概要版)

平成 28 年 8 月 29 日

## はじめに

### (1) 経緯

近年、政府機関を標的とするサイバー攻撃が増加している状況において、環境省も例外ではなくサイバー攻撃が増加しており、平成 27 年度にはサイバー攻撃によりパソコンがマルウェアに感染するなどの事態が発生した。

このように、環境省における現在のセキュリティ・ITに係る体制・対策はまだまだ脆弱な面がある。よって、サイバー攻撃が増加し、脅威が顕在化してきている現況においては、頻繁に職員が入れ替わる組織特性（他府省との人事交流、自治体との人事交流、民間との官民交流等）も踏まえつつ、セキュリティ・ITに係る統括部局の集中的且つ安定的な強化・整備及び有効であり且つ実効性のある取組が必要となっている。

### (2) 目的

本計画は、環境省で所管する情報システムが環境情報の収集・分析・整理・提供の基盤、原子力規制・防災情報の収集・分析・整理・提供の基盤、更には政策の企画・立案、法令案その他公文書類の作成などの行政事務の遂行として重要であることを踏まえ、平成 28 年度から平成 31 年度の 4 年間を対象に、情報システムの適切な運用管理とサイバーセキュリティ対策の指揮監督をする組織として、サイバーセキュリティ・情報化審議官の統括の下、省内における横断的なセキュリティ・ITに係る対策等を強力に推進する体制を整備し、その体制を担う人材として、サイバーセキュリティ及びITに関する一定の専門性を有する人材の育成・確保を図ることを目的に、以下のとおり「環境省におけるセキュリティ・IT人材確保・育成計画」として策定したものである。

環境省では、本計画の着実な実施に向けて取り組むものとし、セキュリティ・IT人材の確保・育成状況等を踏まえ、必要に応じて、適切かつ柔軟に本計画の見直しを行っていくこととする。

## 1. 体制の整備と人材の拡充

環境省では、これまで主として官民交流等によりサイバーセキュリティ及びITに関する専門性を有する人材を確保しているのが現状であったが、平成 28 年度に情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等

について、最高情報セキュリティ責任者（CISO）と情報化統括責任者（CIO）を補佐し、省内の指揮監督できる強力な体制を構築するために、サイバーセキュリティ・情報化審議官を設置したことを踏まえ、セキュリティ・ITに係る統括部局の体制の強化・整備を図るため、ICTに係る業務改革（ワークスタイル変革）、情報システム改革及びサイバーセキュリティ対策の推進を重視し、必要な機構・定員要求を行う。

なお、人材の拡充及び能力の向上のために今後4年間において、セキュリティ・ITに係る統括部局及び情報システムを整備・管理する部局の職員に対する情報システムの整備・管理及び情報セキュリティに関する研修の実施等を行うとともに、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）、内閣官房情報通信技術（IT）総合戦略室（以下「IT室」という。）への職員の出向を行う。

## 2. セキュリティ・IT人材育成支援プログラム

セキュリティ・ITに係る統括部局と情報システムを整備・管理する部局では、そのポストに応じ、情報システムの開発、運用及びセキュリティ対策等に関して実践すべき業務内容・範囲は様々であり、当該業務に対応できる能力を身につける必要がある。また、キャリアパスの中でこれらの様々な能力を身につけた職員が「橋渡し人材」となり、高い職責で現場を指揮・指導していくこととなる。

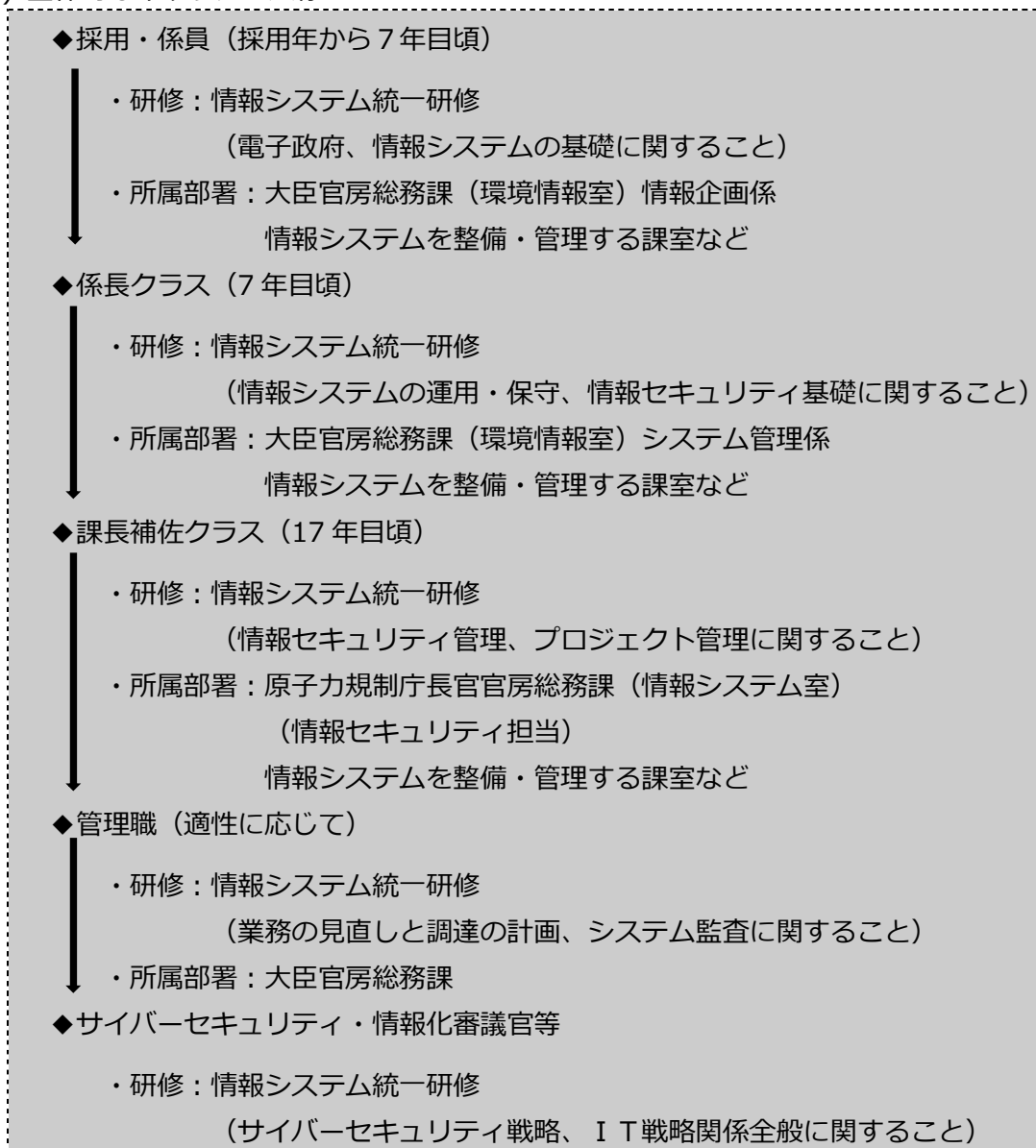
このことから、環境省では、以下の点を重点的に取り組むことにする。

- ▶ セキュリティ・ITに係る統括部局に従事する者には、情報システムの整備・管理におけるITマネジメント及び情報セキュリティマネジメントに関する研修を受講させ、ここで得た知識をベースに、実業務でのOJTにより必要スキルを習得させる。
- ▶ 情報システムを整備・管理する部局に従事する者には、情報システムの設計・開発・運用・保守（改修等）におけるプロジェクト管理及び情報セキュリティ対策に関する研修を受講させ、ここで得た知識をベースに、実業務でのOJTにより必要スキルを習得させる。

また、出向等については、出向先における定員確保を前提に、サイバーセキュリティに係る専門性を有する者の育成についてはNISCに、情報システムの整備・管理に係る専門性を有する者の育成についてはIT室に、それぞれ本計画期間内に数名程度を派遣する。

### 3. 人事ルート例（キャリアパスのイメージ）

#### (1) 全体的なキャリアパス像



#### (2) キャリアパスに含めることが想定される部署

環境省において、情報システムやサイバーセキュリティ対策に係る部署として職員の配属が想定される部署は次の通りである。

- ① セキュリティについて経験することが想定される部署
  - i) 大臣官房総務課（環境情報室）
  - ii) 原子力規制庁長官官房総務課（情報システム室）
  - iii) 情報システムを整備・管理する課室
- ② 情報システム・業務改革について経験することが想定される部署

- i) 大臣官房秘書課
  - ii) 大臣官房総務課（環境情報室）
  - iii) 原子力規制庁長官官房総務課（情報システム室）
- ③ 事案対処、保安、事故対応、危機管理、安全保障等について経験することが想定される部署
- i) 原子力規制庁
    - 長官官房放射線防護グループ
      - 原子力災害対策・核物質防護課
      - 原子力災害対策・核物質防護課核セキュリティ・核物質防護室
      - 原子力災害対策・核物質防護課事故対処室
      - 監視情報課
      - 放射線対策・保障措置課放射線対策規制室
    - 原子力規制部
      - 原子力規制企画課
      - 安全規制管理官（BWR、PWR、新型炉・試験研究炉・廃止措置、再処理・加工・使用、廃棄物・貯蔵・輸送、地震・津波安全対策）付

#### 4. 一般職員の情報リテラシー向上

環境省では、情報セキュリティ及びシステム利用に関する一般行政職員のリテラシー向上のため、次の研修等を実施することとしている。

- 全職員向け研修
  - ・研修内容 : 情報セキュリティについて
  - ・受講対象者 : 全職員
- 新規採用（中途採用）職員及び環境省以外からの出向者向け研修
  - ・研修内容 : 情報セキュリティ等について
  - ・受講対象者 : 毎年の新規採用（中途採用）職員及び環境省以外からの出向者
- 全職員向け訓練
  - ・訓練内容 : 標的型メール攻撃を模した訓練
  - ・訓練対象者 : 全職員

## 防衛省セキュリティ・IT人材確保・育成計画（概要）

### 1 策定の趣旨

平成28年度から平成31年度までの4年間を対象とし、「防衛省セキュリティ・IT人材確保・育成計画」を定める。

### 2 現状

防衛省・自衛隊において、サイバーセキュリティ対策及び情報システムの適切な運用管理等を推進していくためには、セキュリティ・IT人材の確保・育成を計画的に推進し拡充を図る必要がある。

### 3 体制整備

#### (1) 平成29年度における機構・定員要求

防衛省においてサイバーセキュリティ・ITを所管する整備計画局情報通信課の体制を次のとおり整備・強化する。

##### ア 総括班の新設

総括班を新設し、サイバーセキュリティ及びITに関連する各施策を横断的に整理、検討する体制を構築する。

##### イ 情報化推進室への改組等

情報システム室を「情報化推進室」に改組し、防衛省における行政情報化を推進する体制を整備する。

##### ウ 人事・給与等業務の改革

防衛省人事・給与情報システムに係る定員を新たに要求し、当該システムの効率的かつ効果的な整備を行う。

##### エ サイバーセキュリティ体制の強化

- サイバー攻撃に関する情報の収集及び情報通信ネットワーク等の監査に係る業務を行う定員を新たに要求する。
- 防衛産業等のサイバーセキュリティの向上に向けた取組みを支援するための定員を新たに要求し、防衛省と防衛産業等が連携してサイバーセキュリティを強化する体制を整備する。
- 外部の高度専門人材の活用等の企画・立案に携わる定員を増員し、セキュリティ人材の効果的かつ効率的な確保・育成に努める。
- サイバーセキュリティに関する多国間の交流を所掌する定員を増員し、他国との連携強化を推進する体制を強化する。

#### (2) 平成30年度以降の体制整備

サイバーセキュリティ対策及び情報システムの適切な管理等を推進するた

め、整備計画局情報通信課の体制を引き続き整備・強化する。

#### 4 「橋渡し人材」の確保・育成

##### (1) 防衛省・自衛隊における「橋渡し人材」

情報保証制度の制定等、システム利用者とシステム管理者あるいは設計者等との間に立ち、セキュリティレベルの確保やシステム運用の利便性・柔軟性の向上を実現する役割を担う人材を、防衛省・自衛隊における「橋渡し人材」とする。

##### (2) 「橋渡し人材」の確保

- 平成29年度以降、新規採用職員のうち、セキュリティ・ITに関する学位や資格を有する者から、毎年数名程度を「橋渡し人材」候補とし、初年度からセキュリティ・IT関連部署及びその他の行政部署をバランス良く経験させる。
- その後、資質が認められれば、係長昇格時から「橋渡し人材」としてのキャリアパスを踏ませる。
- その他の職員についても、係長昇格時に、その時点においてセキュリティ・ITに関する学位や資格を有し、さらに行政的な能力があると認められる者を、毎年数名程度、「橋渡し人材」に選抜する。

##### (3) 「橋渡し人材」の育成支援プログラム

- 「橋渡し人材」には整備計画局情報通信課等の「橋渡しポスト」での勤務を基本とした上で、所管行政に関する十分な知識を養う機会として行政部署での勤務を、セキュリティ・ITに関する専門性を養う機会として専門部署での勤務を経験させる。
- 内閣官房や総務省が用意する研修や国内外の大学院への留学等を活用することにより、より高度な専門性の習得を図ることとする。

#### 5 職員のリテラシー向上

従来の教育に加え、一般職員を対象とした標的型攻撃メール訓練や段階的なIT及びセキュリティに関する教育（集合教育、eラーニング）を実施し、防衛省における情報リテラシーの一層の向上を図る。

以上