DM2-02-071

別紙１：雛形

# 人事異動等の際に行うべき情報セキュリティ対策実施規程

# 雛形

2007 年 11 月

**内閣官房情報セキュリティセンター**

## 本書の位置付け

本書は、「人事異動等の際に行うべき情報セキュリティ対策実施規程」を策定する場合の雛形であり、「人事異動等の際に行うべき情報セキュリティ対策実施規程 策定手引書」の 2 に示す規程に記載すべき事項を、同 3 に示す文書構成例の枠組みの中に記載したものである。

## 本書の利用方法

### 本書において想定する前提

本雛形は、以下を前提として記述している。そのため、人事異動等の広報の方法、時期、範囲等が以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 人事異動等は、実施の一週間程度前に人事担当課から府省庁内に広報される。
- 各課室の庶務担当者がこれを把握し、情報セキュリティに係る体制において定められた者に通知することができる。
- 行政事務従事者の転入に際して、安全区域への立ち入り及び情報システムを利用するための権限の付与等、業務の実施に必要な情報セキュリティに係る措置は、当人の申請なく行われる。

### 手直しポイント

「人事異動等の際に行うべき情報セキュリティ対策実施規程」の策定にあたり、以下の点について手直しをする必要がある。

① 雛形において*[・・・]* 形式で示す設定値（組織名、期間等）は、各府省庁の定めに合わせる。
② 雛形において【・・・の場合】形式で示す記述については、各府省庁の判断により適宜、選択又は修正する。
③ 既存の人事関連その他の規定との整合性を考慮し、適切に統合、相互参照する。
④ 雛形に記載した［2.1.1(1)(c)］等の項番は、「政府機関の情報セキュリティ対策のための統一基準(第２版)」(NISD-K303-071) の該当する項番である。雛形を利用して策定する規程には、含めなくてよい。

**改訂履歴**

| 改訂日 | 改訂理由 |
|---|---|
| 2006/3/31 | 初版 |
| 2006/8/4 | 誤記訂正 |
| 2007/11/9 | 政府機関統一基準(第２版)の策定に伴う修正 |

# 目次

# 1　本規程の目的

*［○○省］*における情報セキュリティ対策は、それに係るすべての行政事務従事者が、その職制及び職務に応じて与えられている権限と責務を理解した上で、*［省庁対策基準］*及び関連する実施手順に基づき、負うべき責務を全うすることで適切に実施される。このため、それを実施するための基礎となる組織・体制については、行政事務従事者の採用、退職、配置換え等が行われた際においても、適切に整備されている必要がある。さらに、適切に整備された組織・体制の下で、行政事務従事者に対する情報セキュリティに係る教育、権限の付与及び失効等を適時に行うことが情報セキュリティを確保する上で不可欠である。

本規程は、人事異動等に伴い情報セキュリティの観点から行う手続を定め、もって*［○○省］*における情報セキュリティの確保に資することを目的とする。

# 2　適用範囲

## 2.1　本規程の対象者

本規程は、最高情報セキュリティ責任者、情報セキュリティ監査責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者、課室情報セキュリティ責任者、権限管理を行う者、庶務担当者及びすべての行政事務従事者について、それぞれの役割において行うべき措置を定める。

補足：本規程においては、すべての行政事務従事者は原則として課室に属し、情報セキュリティ対策の実施について課室情報セキュリティ責任者等の支援を受けることができるものと想定している。このため、課室に属さない幹部等においては、支援を担当する課室情報セキュリティ責任者等を便宜的に定めた上で本規程を適用する必要がある。

## 2.2　本規程を適用する人事異動等の範囲

本規程は、人事異動発令に基づく採用、退職、配置換え等における情報セキュリティ対策を定めるものである。

なお、本規程では、採用及び他課からの配置換えをあわせて「転入」といい、退職及び他課への配置換えをあわせて「転出」といい、転入と転出をあわせて「人事異動等」という。

*【規程利用者への補足説明】*

*府省庁の運用により、人事発令を伴わない職務の変更により、権限の付与及び失効その他の情報セキュリティ対策の実施が求められる状況が生ずる場合がある。このため、必要に応じて、職務の変更に係る情報を把握する者及び手順を追加又は変更し、府省庁の運用にあわせた規程とすること。*

## 3　人事異動等の把握と通知

(1) 人事異動等の情報は、各課室の庶務担当者が把握する。

(2) 各課室の庶務担当者ごとに、人事異動等の情報を通知する先の者を別表 1 のとおりに定める。

(3) 別表 1 は、統括情報セキュリティ責任者が作成し、常に最新の内容に維持する。

（別表 1 は各課室の庶務担当者ごとに人事異動等の情報を通知する先の者を一覧で示すものであるが、本雛形では省略している。最高情報セキュリティ責任者、情報システム監査責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者、課室情報セキュリティ責任者及び権限管理を行う者にもれなく通知されるように、庶務担当者ごとに通知先の者を定める。）

(4) 各課室の庶務担当者は、把握した課室員の人事異動等の情報を、*［原則として即日、］*別表 1 に記載する者*［全員］*に通知すること。

## 4　人事異動等に伴う措置

人事異動等の情報の通知を受けた者は、以下の措置を採ること。

### 4.1　最高情報セキュリティ責任者が行う措置

#### 4.1.1　特定の責任者等の転出に伴う措置

(1) 情報セキュリティ対策に係る体制の維持

最高情報セキュリティ責任者は、以下の者の転出に際して、後任者を指名すること。

- 最高情報セキュリティアドバイザー［2.1.1(1)(c)］
- 情報セキュリティ委員会委員長及び委員［2.1.1(2)(a)］
- 情報セキュリティ監査責任者［2.1.1(3)(a)］
- 統括情報セキュリティ責任者、情報セキュリティ責任者［2.1.1(4)(a)］
- 情報セキュリティに関する障害等に備えた体制に含まれる者［2.2.2(1)(a)］

### 4.2　情報セキュリティ監査責任者が行う措置

#### 4.2.1　情報セキュリティに係る体制の維持

(1) 情報セキュリティ監査実施者の転出

情報セキュリティ監査責任者は、情報セキュリティ監査実施者の転出に際して、後任者を指名すること。［2.3.2(4)(a)］

### 4.3　統括情報セキュリティ責任者が行う措置

#### 4.3.1　特定の責任者等の転出に伴う措置

(1) 連絡網の維持

統括情報セキュリティ責任者は、情報セキュリティ責任者、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の転出に際して、後任者を確認し、連絡網を更新すること。［2.1.1(4)(f)、(5)(d)、(7)(d)］

(2) 緊急連絡網の維持

統括情報セキュリティ責任者は、特に重要と認めた情報システムについて整備している緊急連絡網に記載した情報システムセキュリティ責任者、情報システムセキュリティ管理者又はその他の者の転出に際して、後任者を確認し、緊急連絡網を更新すること。［2.2.2(1)(d)］

## 4.4 情報セキュリティ責任者が行う措置

### 4.4.1 特定の責任者等の転出に伴う措置

(1) 情報セキュリティに係る体制の維持

情報セキュリティ責任者は、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の転出に際して、後任者を指名すること。また、後任者を統括情報セキュリティ責任者に報告すること。［2.1.1(5)(a)、(5)(c)、(7)(a)、(7)(c)］

## 4.5 情報システムセキュリティ責任者が行う措置

### 4.5.1 行政事務従事者の転入に伴う措置

(1) 電子計算機を管理する行政事務従事者及び利用者を特定するための文書への登録

情報システムセキュリティ責任者は、転入する行政事務従事者に電子計算機を管理又は利用させるに際して、電子計算機を管理する行政事務従事者及び利用者を特定するための文書に必要な事項を反映し、また、当該変更の記録を保存すること。［5.2.1(2)(d)］

(2) 通信回線又は通信回線装置を管理する行政事務従事者を特定するための文書への登録

情報システムセキュリティ責任者は、転入する行政事務従事者に通信回線又は通信回線装置を管理させるに際して、通信回線及び通信回線装置を管理する者を特定するための文書に必要な事項を反映し、また、当該変更の記録を保存すること。［5.4.1(2)(c)］

(3) 通信回線の利用の管理

情報システムセキュリティ責任者は、行政事務従事者の転入に際して、当該行政事務従事者に通信回線を利用させる場合には、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードの対応、及び通信回線の利用部局を含む事項を管理するための文書に、当該転入に伴う変更を反映すること。［5.4.1(2)(a)］

【安全区域へ立ち入る者を承認する手続を整備している場合（強化遵守事項）】

(4) 安全区域立入者の登録

情報システムセキュリティ責任者は、安全区域へ立ち入る者を承認する手続を整備している場合であって、転入する行政事務従事者を安全区域に継続的に立ち入る者として承認するときは、氏名、所属、承認日、期間及び承認事由を含む事項を定められた文書に記録すること。［5.1.1(1)(f)、(1)(g)］

【安全区域へ立ち入る者及び当該区域から退出する者の主体認証を行うための措置を講じている場合（強化遵守事項）】

（例えば、身分証明カードとセキュリティドアによる入退室管理を行っている場合）

(5) 安全区域の認証のための措置への登録

情報システムセキュリティ責任者は、安全区域へ立ち入る者又は当該区域から退出する者の主体認証を行うための措置を講じている場合であって、転入する行政事務従事者に安全区域への立入りを許可するときは、当該措置において立ち入りを許可する者として登録すること。［5.1.1(1)(c)、(1)(d)］

### 4.5.2 特定の責任者等及び行政事務従事者の転出に伴う措置

(1) 情報システムセキュリティ管理者の転出

情報システムセキュリティ責任者は、情報システムセキュリティ管理者の転出に際して、後任者を指名すること。また、後任者を統括情報セキュリティ責任者に報告すること。［2.1.1(6)(a)、(6)(c)］

(2) 権限管理を行う者の転出

情報システムセキュリティ責任者は、権限管理を行う者の転出に際して、後任者を指名すること。［4.1.3(2)(c)］

(3) 電子計算機を管理する行政事務従事者及び利用者の登録削除

情報システムセキュリティ責任者は、電子計算機を管理する行政事務従事者又は利用者として登録された行政事務従事者の転出に際して、*［遅滞なく／転出後○就業日以内に］*、電子計算機を管理する行政事務従事者及び利用者を特定するための文書に反映し、また、当該変更の記録を保存すること。［5.2.1(2)(d)］

(4) 通信回線又は通信回線装置を管理する行政事務従事者の登録削除

情報システムセキュリティ責任者は、通信回線又は通信回線装置を管理する者として登録された行政事務従事者の転出に際して、*［遅滞なく／転出後○就業日以内に］*、通信回線又は通信回線装置を管理する者を特定するための文書に反映し、また、当該変更の記録を保存すること。［5.4.1(2)(c)］

(5) 通信回線の利用の管理

情報システムセキュリティ責任者は、行政事務従事者の転出に際して、当該行政事務従事者に通信回線を利用させていた場合には、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードの対応、及び通信回線の利用部局を含む事項を管理するための文書に、当該転出に伴う変更を反映すること。［5.4.1(2)(a)］

【安全区域へ立ち入る者を承認する手続を整備している場合（強化遵守事項）】

(6) 安全区域立入者の登録削除

情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を承認する手続を整備している場合は、安全区域に継続的に立ち入る者として承認した行政事務従事者の転出に際して、*［遅滞なく／転出後○就業日以内に］*、氏名、所属、承認日、期間及び承認事由を含む事項を記録した文書に必要な事項を反映し、当該変更の記録を保存すること。［5.1.1(1)(g)］

【安全区域へ立ち入る者の主体認証を行うための措置を講じている場合（強化遵守事項）】

（例えば、身分証明カードとセキュリティドアによる入退室管理を行っている場合）

(7) 安全区域認証の登録削除

情報システムセキュリティ責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講じている場合は、安全区域への立入りを許可している行政事務従事者の転出に際して、*［遅滞なく／転出後○就業日以内に］*、当該措置における登録を削除すること。［5.1.1(1)(c)、(1)(d)］

(8) 府省庁外での情報処理のための機器の返却
　情報システムセキュリティ責任者は、府省庁外での情報処理を行っている行政事務従事者の転出に際して、端末、外部記録媒体等の返却を含む当該情報処理を終了するときの手続に従った措置を講じさせること。［6.2.1(2)(d)、(2)(e)、(2)(j)、(2)(k)、(3)(b)、(3)(d)］

(9) 府省庁支給以外の情報システムによる情報処理に関する情報の消去
　情報システムセキュリティ責任者は、府省庁支給以外の情報システムによる情報処理を行っている行政事務従事者の転出に際して、情報の消去を含む当該情報処理を終了するときの手続に従った措置を講じさせること。［6.2.2(2)(d)、(2)(e)、(3)(b)］

## 4.6　課室情報セキュリティ責任者が行う措置

### 4.6.1　行政事務従事者の転入に伴う措置

(1) 転入者への教育
　課室情報セキュリティ責任者は、行政事務従事者の転入に際して、3 か月以内に情報セキュリティ対策の教育を受講させること。［2.2.1(1)(d)、(1)(g)］

### 4.6.2　行政事務従事者の転出に伴う措置

(1) 府省庁外での情報処理のための機器の返却
　課室情報セキュリティ責任者は、府省庁外での情報処理を行っている行政事務従事者の転出に際して、端末、外部記録媒体等の返却を含む当該情報処理を終了するときの手続に従った措置を講じさせること。［6.2.1(2)(d)、(2)(e)、(2)(j)、(2)(k)、(3)(b)、(3)(d)］

(2) 府省庁支給以外の情報システムによる情報処理に関する情報の消去
　課室情報セキュリティ責任者は、府省庁支給以外の情報システムによる情報処理を行っている行政事務従事者の転出に際して、情報の消去を含む当該情報処理を終了するときの手続に従った措置を講じさせるここと。［6.2.2(2)(d)、(2)(e)、(3)(b)］

## 4.7　権限管理を行う者が行う措置

### 4.7.1　行政事務従事者の転入に伴う措置

(1) 識別コード及び主体認証情報（パスワード等）の付与
　権限管理を行う者は、行政事務従事者の転入に際して、利用させる電子計算機、アプリケーションソフトウェア等について識別コード及び主体認証情報を発行すること。［4.1.3(2)(d)］

(2) 主体認証情報格納装置の交付
　権限管理を行う者は、行政事務従事者の転入に際して、主体認証情報格納装置を利用させる場合には、これを交付すること。［4.1.3(2)(d)］

(3) アクセス制御の設定
　権限管理を行う者は、行政事務従事者の転入に際して、必要最小限の範囲に限って許可を与えるように情報システムにおけるアクセス制御の設定をすること。［4.1.3(2)(i)］

【行政事務従事者と識別コードの対応の記録を保存する場合（強化遵守事項）】

(4) 行政事務従事者と識別コードの対応の記録
　権限管理を行う者は、行政事務従事者の転入に際して、当該行政事務従事者と付与した識別コードの対応を記録し、これを保存すること。［4.1.3(2)(k)］

(5) 識別コード及びアクセス制御設定の見直し
　権限管理を行う者は、人事異動等により識別コードを追加する機会に、不要な識別コード及び不適切なアクセス制御設定の有無を点検すること。［4.1.3(2)(g)、(2)(i)］

#### 4.7.2　行政事務従事者の転出に伴う措置

(1) 識別コードの無効化
　権限管理を行う者は、行政事務従事者の転出に際して、利用させる電子計算機、アプリケーションソフトウェア等について付与していた当該主体の識別コードを*［遅滞なく／転出後○就業日以内に］*無効にすること。［4.1.3(2)(g)］

(2) 主体認証情報格納装置の返還
　権限管理を行う者は、主体認証情報格納装置を交付していた行政事務従事者の転出に際して、当該主体認証情報格納装置を返還させること。［4.1.3(2)(h)］

(3) 識別コード及びアクセス制御設定の見直し
　権限管理を行う者は、人事異動等により識別コードを削除する機会に、不要な識別コード及び不適切なアクセス制御設定の有無を点検すること。［4.1.3(2)(g)、(2)(i)］

### 4.8　行政事務従事者が行う措置

#### 4.8.1　自らの転入に伴う措置

(1) 教育の受講
　行政事務従事者は、自らの転入に際して、情報セキュリティ対策の教育の受講方法について課室情報セキュリティ責任者に確認すること。［2.2.1(2)(b)］

#### 4.8.2　自らの転出に伴う措置

(1) 府省庁外での情報処理のための機器の返却
　府省庁外での情報処理を行っている行政事務従事者は、自らの転出に際して、府省庁外での情報処理を行っていた場合には、端末及び外部記録媒体等の返却を含む当該情報処理を終了するときの手続に従った措置を講ずること。［6.2.1(2)(d)、(2)(e)、(2)(j)、(2)(k)、(3)(b)、(3)(d)］

(2) 府省庁支給以外の情報システムによる情報処理に関する情報の消去
　府省庁支給以外の情報システムによる情報処理を行っている行政事務従事者は、自らの転出に際して、情報の消去を含む当該情報処理を終了するときの手続に従った措置を講ずること。［6.2.2(2)(d)、(2)(e)、(3)(b)］

## 5　履行状況の確認

(1) 履行状況の確認
　情報セキュリティ責任者は、前章までの規定の履行状況を定期的に確認すること。なお、当該確認は、自己点検の一部として行うことをもって代えることがで

きる。［2.1.1(4)(d)］

## 6　本規程に関する相談窓口

(1) 本規程の対象者は、緊急時の対応又は本規程の内容を超えた対応が必要とされる場合には、情報セキュリティ体制の上位者に相談し、指示を受けること。

(2) 本規程の対象者は、本規程の内容について不明な点又は質問がある場合には、情報セキュリティ体制の上位者に連絡し、回答を得ること。