（資料４９）国立環境研究所情報セキュリティポリシーの概要

（第２版：平成 19 年 12 月改訂）

Ⅰ．趣　旨

国立環境研究所情報セキュリティポリシーは、研究所の情報資産をあらゆる脅威（要保護情報の外部への漏洩、外部からのホームページ掲載情報への不正侵入・改ざん等）から守るため、情報セキュリティ対策に関して研究所の全在籍者がその立場に応じて遵守すべき基本的な考え方をとりまとめたものである（平成 18 年 12 月策定）。本ポリシーは「政府機関の情報セキュリティ対策のための統一基準」に準拠して策定することとされており、同統一基準の記述を踏まえたものである。

Ⅱ．本ポリシーの概要

（１）組織と体制の構築

本ポリシー及び本ポリシーに基づく関連規程の策定・見直し等を行うとともに本ポリシーの円滑かつ効果的な運用を図るため、研究所内に次のような組織・体制を構築する。また、これらの体制のもと、研究所の在籍者に対する情報セキュリティ対策教育を実施するなど、本ポリシーの実効性を高める措置を講ずる。

（ａ）最高情報セキュリティ責任者

【役割】研究所における情報セキュリティ対策に関する事務を統括する。

【担当】企画・総務担当理事（ＣＩＯ）

（ｂ）最高情報セキュリティアドバイザー

【役割】最高情報セキュリティ責任者が必要に応じて置く専門家であり、情報セキュリティに関する専門的知識及び経験に基づくアドバイスを行う。

【担当】国立環境研究所ＣＩＯ補佐

（ｃ）情報セキュリティ委員会

【役割】最高情報セキュリティ責任者が設置する所内委員会であり、研究所の情報セキュリティに関するポリシーを策定し、最高情報セキュリティ責任者の承認を得る。

【担当】委員長として企画・総務担当理事（ＣＩＯ）、副委員長として環境情報センター長及び委員として各ユニット長

（ｄ）情報セキュリティ監査責任者

【役割】最高情報セキュリティ責任者が置くもので、最高情報セキュリティ責任者の指示に基づいて監査に関する事務を統括する。

【担当】監査室長

（ｅ）統括情報セキュリティ責任者

【役割】（ｆ）の情報セキュリティ責任者のうちから最高情報セキュリティ責任者が１人を置くもので、情報セキュリティ責任者を統括する。

【担当】環境情報センター長

（ｆ）情報セキュリティ責任者

【役割】最高情報セキュリティ責任者が定める情報セキュリティ対策の運用に係る管理を行う単位ごとに各１人を置くもので、所管する単位における情報セキュリティ対策に関する事務を統括する。

【担当】各ユニット長

（ｇ）情報システムセキュリティ責任者

【役割】情報セキュリティ責任者が所管する単位における情報システムごとに置くもので、所管する情報システムに対する情報セキュリティ対策の管理に関する事務を統括する。

【担当】情報システムを有する課室の長

（ｈ）情報システムセキュリティ管理者

【役割】情報セキュリティ責任者が所管する単位における情報システムごとに置くもので、所管する情報システムの管理業務における情報セキュリティ対策を実施する。

【担当】各情報システムの管理運用担当者

（ｉ）課室情報セキュリティ責任者

【役割】情報セキュリティ責任者が所管する課室ごとに置くもので、所管する課室における情報セキュリティ対策に関する事務を統括する。

【担当】各課室の長

（２）情報についての対策（主たる対象者：業務従事者）

（ａ）情報の格付け

取り扱うすべての情報について、機密性、完全性及び可用性の観点から格付けを行う（書面については機密性のみ）。

〇機密性：情報に対してアクセスを認可された者だけがこれにアクセスできる状態を確保すること。

〇完全性：情報が破壊、改ざん又は消去されていない状態を確保すること。

〇可用性：情報へのアクセスを認可された者が、必要時に中断することなく情報及び関連資産にアクセスできる状態を確保すること。

情報の格付け（１）

ﾗﾝｸ	機密性	完全性	可用性
１	機密性２及び３以外の情報	完全性２以外の情報	可用性２以外の情報
２	業務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより、国民の権利が侵害され又は業務の遂行に支障を及ぼすおそれがある情報	業務で取り扱う情報のうち、その改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適確な遂行に支障を及ぼすおそれがある情報	業務で取り扱う情報のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障を及ぼすおそれがある情報
３	秘密文書に相当する機密性を要する情報		

情報の格付け（２）

ﾗﾝｸ	機密性	完全性	可用性
１			
２	**要機密情報**	**要保全情報**	**要安定情報**
３			

※上記の網掛け部分の情報全体を「要保護情報」という。

（ｂ）情報の利用、保存、移送、提供、消去

上記の格付けに応じて、それぞれの情報に次のような取扱制限を明記する。

〇情報の利用：利用者の制限や複製・配布の制限等

〇情報の保存：適切なアクセス制限や記録媒体の管理、保存期間の設定等

〇情報の移送：情報の外部への移送手段や適切な安全確保措置等の確保及びそれらを実施するに当たり事前の責任者の許可体制の確立等

〇情報の提供：機密性１以外の情報の公開禁止の確認措置及び要機密情報を外部に提供するに当たり事前の責任者の許可体制の確立等

〇情報の消去：電磁的記録及び書面での記録を廃棄する際の方法等

（３）情報セキュリティ要件の明確化に基づく対策（主たる対象者：情報システムセキュリティ責任者及び情報システムセキュリティ管理者）

（ａ）主体認証、アクセス制御、権限管理、証跡管理機能

すべての情報システムについて主体認証（パスワードの設定等）、アクセス制御（当該情報システムの利用許可等）、権限管理機能（当該情報システムの管理者としての権限の付与等）、証跡管理機能（アクセスログ取得等）の必要性の有無を検討し、必要と認めたものにはそれぞれの機能を設定の上、適切な管理を行うなど必要な措置を講ずる。要保護情報を取り扱う情報システムは、主体認証、アクセス制御及び権限管理の各機能の必要性有りとする。

（ｂ）暗号と電子署名

要機密情報を取り扱う情報システムについては暗号化機能を、要保全情報を取り扱う情報システムについては電子署名機能をそれぞれ付加する必要性の有無を検討し、必要と認めたものには機能を設定の上、適切な管理を行うなど必要な措置を講ずる。

（ｃ）情報セキュリティについての脅威

情報システムのセキュリティホール、コンピュータウィルスなどの不正プログラム、外部からのサービス不能攻撃（ホームページ等への不正侵入等）等の情報セキュリティについての脅威に対して、情報システムの構築時及び運用時の両場面において適切な対策を講ずる。

（４）情報システムの構成要素についての対策（主たる対象者：情報システムセキュリティ責任者及び情報システムセキュリティ管理者）

（ａ）電子計算機及び通信回線装置を設置する安全区域の設定

必要に応じて電子計算機及び通信回線装置を設置するための物理的な安全区域の設定（セキュリティ、災害、障害等対応）を設定するとともに、設定した安全区域には不審者を始め無許可の者を立ち入らせない措置を講ずる。

（ｂ）電子計算機、端末、サーバ装置、アプリケーション（電子メール、ウェブ）、接続通信回線の個別対策

電子計算機等のハードウェア及びアプリケーション等のソフトウェアのそれぞれについて、個別にセキュリティ維持に関する対策を講ずる。ハードウェアに関してはそれぞれのシステムごとに主体認証機能（パスワード等）や権限管理等の必要な設定を行い、ソフトウェアに関しては適切なコンピュータウィルス対策やシステムのセキュリティホール対策等を講ずる。

（５）個別事項についての対策（主たる対象者：業務従事者）

機器調達（リース等を含む。）・ソフトウェア開発等の外部委託を要する案件についての安全管理について規定するとともに、委託業者に対して必要なセキュリティ対策の設定を求める。研究所外において要保護情報を取り扱うような案件については、特にその安全管理措置を講ずるとともに、委託業者に対しても同様な措置を求める。