

高エネルギー加速器研究機構 情報セキュリティポリシー

平成18年12月改訂
平成16年4月
高エネルギー加速器研究機構

1. セキュリティポリシー基本方針

高度情報社会において、高エネルギー加速器研究機構（以下、「機構」という。）が研究・業務を遂行するためには、情報基盤の整備に加えて、大学共同利用機関法人にふさわしい情報セキュリティ水準を達成することが不可欠である。このため、機構は「情報セキュリティポリシーに関するガイドライン（平成12年7月18日情報セキュリティ対策推進会議決定 平成14年11月28日一部改定）」および「大学における情報セキュリティポリシーの考え方(平成14年3月29日大学の情報セキュリティポリシーに関する研究会)」を踏まえ「高エネルギー加速器研究機構情報セキュリティポリシー」（以下、「ポリシー」という。）を定める。なお、J-PARCセンターの情報セキュリティポリシーは別に定めるものとする。

ポリシーは、次の4項目を基本的な考え方とし、機構の職員および職員に準ずる者ならびに共同利用者等は、ここに定めるセキュリティポリシーを理解し遵守しなければならない。

- ・ 機構内外の情報資産を不正に使用してはならない。
- ・ 自分が使用・管理する情報資産を他に不正に使用させてはならない。
- ・ 情報資産の不正使用を発見した場合は速やかにこれに関する通報と対処を行わなければならない。
- ・ 自分が管理する情報資産に対して、そのセキュリティに責任を負わなければならない。

ここで情報資産とは、電子的に記録された情報およびハードウェア、ソフトウェア、ネットワーク、記憶媒体等で構成される計算機資源(情報システム)を合わせたものである。

2. 対策基準

(1) 組織・体制

(1.1) 最高情報セキュリティ責任者

最高情報セキュリティ責任者は、機構のすべての情報セキュリティに関し、機構内の組織および機構外部に対する責任を負う。

(1.2) 情報セキュリティ責任者

情報セキュリティ責任者は、機構の情報セキュリティ管理の実施に関し、総括的な対応にあたり、最高情報セキュリティ責任者を補佐する。

(1.3) 情報セキュリティ委員会

情報セキュリティ委員会は、機構の情報セキュリティに関する最高審議機関として、機構長の求めに応じて、機構の情報セキュリティにかかわる重要事項を審議するとともに機構の情報セキュリティに関し、機構長に提言することができる。また、具体的な事項を検討するため、本委員会の下に部会を設置することができる。

(1.4) 情報セキュリティポリシー策定部会

情報セキュリティポリシー策定部会は、情報セキュリティ委員会の下に設置され、各研究所・施設等から選出される委員によって構成し、ポリシー案の作成ならびにポリシーについての評価および改訂案の作成等を行う。

(1.5) 情報セキュリティ管理部会

情報セキュリティ管理部会は、最高情報セキュリティ責任者の下に設置され、各研究所・施設等の情報セキュリティマネージャ（3.1.3）および計算科学センター職員若干名で構成し、ポリシーに添った実施手順の作成およびその実施にあたりとともに必要な連絡調整を行う。また、不正アクセス発生時の緊急対応手順を定める。

(2) 情報の分類と管理

本ポリシーにおいて取り扱う情報とは、電子的に記録された情報をいう。情報は、内容に応じて分類され、分類ごとに適切な管理および対応が行われなければならない。

(2.1) 情報の分類

機構で取り扱うすべての情報について、公開・非公開を定めること。

(2.1.1) 公開・非公開の定義

公開とは、情報を管理する責任を負う者（以下、「情報管理責任者」という。）が、情報にアクセスできる者の範囲を限定せずにその情報を開示することをいう。非公開とは、情報管理責任者が、情報にアクセスできる者の範囲を定め、許可された者以外に情報を開示しないことをいう。

(2.1.2) 非公開情報

機構で取り扱うすべての情報は、その作成・発生時点において、その分類を非公開とする。

(2.1.3) 公開情報

非公開情報の分類を公開とするには、当該情報管理責任者の許可を要する。

(2.2) 情報の管理

情報の管理は、当該情報管理責任者がその責任を負う。

(2.2.1) 情報管理責任者

情報管理責任者は、原則的にその情報の作成者とする。

(2.2.2) 非公開情報の管理

- ・ 非公開情報には、アクセス権の設定、暗号化等、必要に応じた制限を設定すること。
- ・ 非公開情報は、物理的な盗難等を防止する措置を講ずること。

(2.2.3) 公開情報の管理

情報管理責任者は、情報の公開にあたっては、以下の事項を遵守するものとする。

- ・ 個人情報の漏洩、プライバシーや著作権の侵害等に十分注意すること。
- ・ 該当する研究所・施設等において公開に関して必要な内部手続きを経ること。
- ・ 情報の改ざんや偽情報の流布に対し必要な防止策を講ずること。
- ・ 公開情報の複製を別に保存すること等により、情報の原本性を維持すること。
- ・ 情報の改ざんを受けることも想定し、情報の速やかな回復機構を備えること。

(2.2.4) 記憶媒体の処分

- ・ 公開・非公開を問わず、情報システムおよび記憶媒体を処分する場合は、そこに保存された情報の消去が確実に行われるよう、その処分方法に十分注意すること。
- ・ 公開・非公開を問わず、情報システムおよび記憶媒体を保守契約により交換する場合は、撤去後の記憶媒体の処分方法について十分注意しなければならない。レンタルシステムの場合についても同様とする。

(3) 人的セキュリティ

(3.1) 役割・責任

(3.1.1) 最高情報セキュリティ責任者

- ・ 最高情報セキュリティ責任者は、高度情報利用推進室長をもって充てる。
- ・ 最高情報セキュリティ責任者は、情報セキュリティ委員会で承認されたポリシーに基づき、機構のすべての情報セキュリティに関する権限と責任を有する。
- ・ 最高情報セキュリティ責任者は、情報システムの円滑な運用に必要な措置を情

報セキュリティ責任者に指示し、緊急避難措置に対処する。

- ・ 最高情報セキュリティ責任者は、情報セキュリティに関する外部からの苦情への対応（損害賠償請求など法的対応部署との連携を含む。）ならびに外部から受けた被害への対応（被害回復請求など）にあたる。
- ・ 最高情報セキュリティ責任者は、情報セキュリティ責任者による定常的なセキュリティ対策の措置ならびにセキュリティ管理の状況に関する報告に対処する。

(3.1.2) 情報セキュリティ責任者

- ・ 情報セキュリティ責任者は、最高情報セキュリティ責任者によって指名される。
- ・ 情報セキュリティ責任者は、情報セキュリティ管理部会において主査を務め、実施手順の作成および実施に関する協議を進める。
- ・ 情報セキュリティ責任者は、機構の情報システムが円滑に運用されるように、情報セキュリティの保持と強化のための技術的な調査検討を行うとともに、緊急時の総括的な連絡窓口として機能する。
- ・ 情報セキュリティ責任者は、情報セキュリティを守るために必要な緊急避難措置をとることができる。ただし、その措置の影響を受ける情報システムのシステム管理者(3.1.4)または情報管理責任者に、その旨を速やかに通知しなければならない。対応策の実施が完了したと判断した場合は、緊急避難措置を解除する。情報セキュリティマネージャ(3.1.3)、システム管理者および情報管理責任者から緊急避難措置の依頼があった場合も同様に扱うものとする。
- ・ 情報セキュリティ責任者は、機構の情報セキュリティの管理および監査の実施に関し、最高情報セキュリティ責任者を補佐し、必要な技術的措置を提案する。

(3.1.3) 情報セキュリティマネージャ

- ・ 情報セキュリティマネージャは、各研究所・施設等内における情報セキュリティポリシーの実施に関する権限と責任を有し、各研究所・施設等内に情報セキュリティに関する連絡体制を構築し、ポリシーの遵守に関する意見の集約を行う。
- ・ 情報セキュリティマネージャは、情報セキュリティ管理部会において情報セキュリティの保持と強化のための技術的な調査検討を行い、セキュリティ対策の実施にあたる。
- ・ 情報セキュリティマネージャは、システム管理者に対し情報システムの円滑な運用のために必要な技術的措置を提案・助言する。
- ・ 情報セキュリティマネージャは、各研究所・施設等内において情報セキュリティを守るために必要と判断したときは、緊急避難措置をとることができる。緊急避難措置をとった場合には、情報セキュリティ責任者および情報セキュリティ管理部会にその事実を速やかに報告すること。

(3.1.4) システム管理者

- ・ システム管理者は、自ら管理する情報システムに関して利用資格を定めること。
- ・ システム管理者は、自ら管理する情報システムに関して設定の変更、運用、更新等を行う権限と責任を有する。
- ・ システム管理者は、自ら管理する情報システムに関してポリシーを遵守するために必要な措置を講ずる責任を有する。
- ・ システム管理者は、情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者も含めて、ポリシーを十分に説明すること。受注者は、ポリシーを遵守すること。

(3.1.5) 情報管理責任者

- ・ 情報管理責任者は、原則的にその情報の作成者とする。
- ・ 複数人で作成した情報の情報管理責任者は、その代表者とする。
- ・ その他必要に応じて、上位の者を情報管理責任者とすることができる。
- ・ 情報管理責任者は、管理する情報の公開・非公開を決定することができる。
- ・ 情報管理責任者は、公開情報及び非公開情報についての管理責任を有し、その管理にあたっては、ポリシーを遵守しなければならない。

(3.1.6) 一般利用者（職員および職員に準ずる者ならびに共同利用者等）

- ・ 一般利用者は、ポリシーおよびシステム管理者がポリシーを遵守するために必要とする措置を遵守しなければならない。
- ・ 一般利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合、それについて速やかに該当する研究所・施設等内の情報セキュリティマネージャに相談し、指示等を仰ぐこと。

(3.2) 啓発およびポリシーの周知

- ・ 情報セキュリティ管理部会は、必要に応じてポリシーに関する説明会を実施し、システム管理者、一般利用者および情報管理責任者に対しポリシーについて啓発すること。
- ・ 情報システムを利用するすべてのものは、研修会や説明会等を通じ、ポリシーおよび実施手順を理解し、情報セキュリティ上の問題が生じないように努めること。

(3.3) 不正アクセスの報告

- ・ 一般利用者は、情報システムの不審な動作、公開情報の改ざんを発見した場合

は、該当するシステム管理者または情報管理責任者に直ちに報告すること。

- ・ システム管理者は、情報セキュリティに関する事故の発生時には、事故を分析し、再発防止のための情報として記録を保存すること。また、事故を、該当する研究所・施設等の情報セキュリティマネージャに直ちに報告すること。
- ・ 情報セキュリティマネージャは、事故を情報セキュリティ管理部会に直ちに報告し、必要に応じて情報セキュリティ責任者に、対処に関しての指示または支援を要請できる。
- ・ 情報セキュリティ責任者は、その重要性に応じてこれらの事故を最高情報セキュリティ責任者に報告する。
- ・ 外部者から、機構の情報システムに関する事故、システム上の欠陥及び誤動作等に関する情報提供を受けた場合も同様とする。

(3.4) アクセスのための認証情報等の管理

個人を認証するためのパスワードや認証用のハードウェア (ICカード、トークン等) の管理については、一般利用者およびシステム管理者は以下の事項を遵守するものとする。

(3.4.1) 一般利用者の認証情報等の管理

- ・ 一般利用者は、自己のパスワードを秘密とすること。また、十分なセキュリティを維持できるよう、自己のパスワードの設定および変更配慮すること。
- ・ 一般利用者は、他の利用者のアカウントを使用してはならない。
- ・ 情報システムのシステム管理者が、パスワードの変更を求めた場合、その利用者はその指示に従うこと。
- ・ 情報システムの利用者は、システム管理者および第三者からのパスワードの聞き取りに対して、いかなる場合も応じてはならない。
- ・ 情報システムの利用者は、認証用のハードウェアを、システム管理者の定める事項に従い厳重に管理すること。
- ・ 情報システムの利用者は、認証用のハードウェアを紛失した場合は、直ちにシステム管理者へ届け出ること。

(3.4.2) システム管理者の認証情報等の管理

- ・ システム管理者は、(3.1.4) により規定される利用資格を有する者以外にアカウントを発行してはならない。また、利用資格を失った者のアカウントは、速やかに削除するものとする。
- ・ システム管理者は、利用者のアカウントを管理権限のない第三者に漏洩してはならない。また、いかなる場合も利用者からパスワードを聞き取りしたり、認証

用ハードウェアを預かったりしてはならない。

(4) 技術的セキュリティ

(4.1) ネットワークモニタリング

情報セキュリティ管理部会は、不正アクセスや不正使用を速やかに発見するために、機構内外間の通信をネットワーク・モニタ装置等により、実施手順に従いモニタする。

(4.2) アクセス制御

システム管理者は、情報システムを、計算科学センターが定める手続きに従って機構のネットワークに接続することができる。ネットワークに接続された情報システムは、アクセス制御の方法によって分類される。

(5) 物理的セキュリティ

情報システムの設置場所は、不正な立ち入りを排除する等安全性を保つよう努めなければならない。机上のパソコンまたは持ち運びを前提としたノートパソコン等の情報システムを保護するための対策にも十分配慮すること。

(6) 運用

(6.1) 情報システムの監視

- ・ システム管理者は、セキュリティに関する事案を検知するため、常に管理する情報システムの監視を行うこと。
- ・ システム管理者は、監視により得られた結果を、消去や改ざんをされないために必要な措置を施し、定期的に安全な場所に保管すること。また、これらの記録の正確性を確保するため、情報システムに正確な時刻の設定を行うこと。

(6.2) ポリシーの遵守状況の確認

- ・ 一般利用者は、ポリシー違反を発見した場合、直ちに情報セキュリティマネージャに報告しなければならない。情報セキュリティマネージャは、違反が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると判断した場合は、緊急対応手順に従って連絡を行うこと。
- ・ 情報セキュリティマネージャは、該当する研究所・施設等内におけるポリシーの実施状況を確認すること。
- ・ 情報セキュリティ責任者は、情報セキュリティ管理部会を定期的に開催し、ポリシーの遵守状況について分析・整理し、その結果を最高情報セキュリティ責任者に報告すること。最高情報セキュリティ責任者は、必要に応じてこれを機構長に報告すること。

(6.3) 利用者の意見

情報セキュリティマネージャは、システム管理者、一般利用者および情報管理責任者からポリシーに関する意見を収集し、情報セキュリティ管理部会に報告すること。

(6.4) セキュリティ診断

情報セキュリティ責任者は、情報システムの機密性、完全性および可用性ならびに犯罪予防の観点から、情報システムに対するセキュリティ診断を実施すること。その結果を情報セキュリティ診断として取りまとめ、最高情報セキュリティ責任者に報告すること。診断過程で重大なセキュリティの脆弱性が発見された場合は、緊急避難措置をとるとともに、システム管理者と該当する研究所・施設等の情報セキュリティマネージャに、その脆弱性の内容および緊急避難措置の内容を速やかに報告すること。

(6.5) セキュリティ監査

情報セキュリティ責任者は、定期および不定期に監査を実施し、各研究所・施設等のポリシーの遵守状況および運用実態を把握し、情報セキュリティ管理部会に報告するものとする。情報セキュリティ管理部会は、報告内容を情報セキュリティ監査結果として取りまとめ、最高情報セキュリティ責任者に報告すること。

(6.6) セキュリティ対策費

最高情報セキュリティ責任者は、情報セキュリティ対策に要した直接的経費を把握すること。また、次年度の情報セキュリティ計画および予算案の検討を行い、機構長に提案すること。

(7) 不正アクセス発生時の対応

情報セキュリティ管理部会は、外部または内部からの不正アクセスが発生した場合、緊急対応手順に従い、関連する通信の遮断または関連する機器のネットワークからの切り離しを実施する。発生した不正アクセスが、緊急対応手順では取り扱えない場合には、情報セキュリティ責任者の指示に従う。

(8) 評価及び見直し

情報セキュリティ委員会は、セキュリティレベルの向上に必要な事柄を審議するため、少なくとも年1回会合をもつ。

(8.1) ポリシーの評価および更新

情報セキュリティ委員会は、ポリシーの実効性を評価し、必要な部分を見直して内

容の変更を行い、よりセキュリティレベルの高いかつ遵守可能なポリシーに更新する。

(8.2) 報告義務

情報セキュリティ委員会は、機構長に評価・見直しの結果を報告すること。

(9) 情報セキュリティに関する違反に対する対応

情報セキュリティ委員会は、ポリシーに違反した者について、その重大性、発生した事案の状況等に応じて処分等を検討する。なお、処分の決定は機構長が行う。

(10) 法令遵守

情報システムの利用者は、使用する情報資産について関連する法令を遵守し、これに従うこと。