広島国際大学情報セキュリティ対策基準

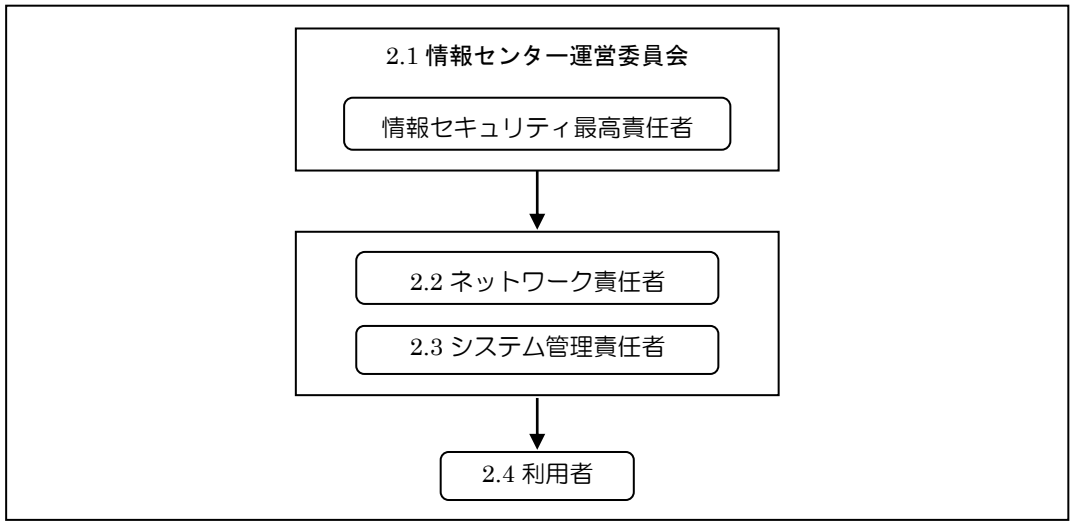
2019 年 7 月 23 日　制定

１．目的

広島国際大学は、情報セキュリティ基本方針に基づき、情報セキュリティの運用・管理を確保するために遵守すべきことについて、人的な側面、物理的な側面および運用・技術的な側面から基準を策定し、本学が保有する情報資産を対象とした情報セキュリティの推進を図る。

２．組織・体制

情報セキュリティの運用・管理の体制を組織化し、その責任と権限を明確にする。



2.1 情報センター運営委員会

情報センター運営委員会は、情報セキュリティポリシーの策定および重要事項の決定を行う。具体的な活動内容は以下の項目とする。

- 情報セキュリティポリシーの策定と評価および見直し。
- 遵守事項の違反等に対する措置。
- 学園内の他の意思決定組織との調整。
- その他、情報セキュリティに関する重要な事項の審議。

2.1.1 情報セキュリティ最高責任者

情報セキュリティ最高責任者は、情報セキュリティポリシーに基づき、学内の情報セキュリティに関する総括的な意思決定にあたる。

2.2 ネットワーク責任者

ネットワーク責任者は、全学の情報システムが円滑に運用されるよう、情報セキュリティの保護とネットワークの維持管理のための具体的な対策を講じる。また、学外からの攻撃、脆弱性が発見された場合は、情報セキュリティ最高責任者に速やかに報告するとともに緊急措置を講じる。

2.3 システム管理責任者

システム管理責任者は、情報機器を保管する部署の責任者をいう。ただし、学部・学科で共有して使用している情報機器はその学部・学科の長をシステム管理責任者とする。システム管理責任者は、該当する各情報機器を維持・管理し、セキュリティを最新の状態に保つよう努めなければならない。

システム管理責任者は、管轄する情報機器を他の利用者（学生、教職員、臨時要員等）にシステム管理業務を委託させる場合は、責任と権限を明確にし、守らせなければならない。

2.4 利用者

利用者は、基本方針の適用範囲に示す者をいう。利用者は、本学の情報セキュリティポリシーを遵守し、情報セキュリティ実施手順に従って情報機器を利用しなければならない。また、システム管理責任者やネットワーク責任者からセキュリティ維持管理のために必要な措置を指示された場合は、直ちにその指示に従わなければならない。

３．情報の管理

3.1 入退室管理

システム管理責任者は、重要な情報が保存されている情報機器等を設置しているコンピュータ室やサーバ室の入退室を厳重に管理しなければならない。また、それ以外の場所においても情報機器の盗難・き損および情報の漏洩・改ざん等が起きないよう必要な対策を講じなければならない。

3.2 情報の開示

システム管理責任者は、学内外のネットワークを利用して情報を開示させる場合に、情報の改ざんや偽情報の流出に対して十分な防止策を講じなければならない。また、情報開示の対象者を特定する場合は、アクセス制限やネットワークの分離等の対策を行い、正当なアクセス権を持たない者に利用されることがないようにしなければならない。さらに、改ざん等により偽情報に書き換えられる場合に備えて、原本性を保証するために速やかな回復機能を用意しておかなければならない。

3.3 情報機器および記憶媒体の処分

システム管理責任者は、情報機器および記憶媒体を廃棄する場合、データ等が第三者に読み取られることのないよう、物理的な破壊や完全消去によりデータの読み取りが不可能な状態にしなければならない。

４．運用および技術的な対応

4.1 情報機器の管理

システム管理責任者は、情報機器のセキュリティを最新の状態に保ち、他からの攻撃を防ぐ対策を講じなければならない。また、万一攻撃等を受けた場合は、速やかに被害の拡大を回避する処置をとらなければならない。また、ネットワークに接続されている情報機器のうち個人データなどの重要な情報が保管されている場合は、ID 認証を設定し利用者のアクセス権限を有効にしておかなければならない。万一、ウイルスに感染したり、外部から攻撃を受けたりした場合は、速やかにネットワークの接続を停止し、必要な対策を講じなければならない。

4.2 アカウントの管理

ネットワーク責任者およびシステム管理責任者は、情報システムの利用にあたって、各システムについて利用資格および利用権限（アカウント）を明確に定めなければならない。また、利用者に対して関連する法令、規定、遵守事項を周知しなければならない。利用資格を消失したアカウントは、速やかにシステムに反映させ、該当アカウントでの利用をさせない等の処置を講じなければならない。利用者は、発行された利用権限の ID とパスワードを他人に使用させてはならない。

4.3 ネットワークにおけるセキュリティ

4.3.1 ネットワークの分離

ネットワーク責任者は、ファイアウォール等の導入により、インターネットと学内 LAN および組織の内外を必要に応じて分離し、不要あるいは不正な情報を通さない仕組みを講じなければならない。

4.3.2 無線ＬＡＮ

システム管理責任者は、無線ＬＡＮを運用する場合に適切なセキュリティ設定を行い、盗聴、情報の改ざん、漏洩および破壊などの重大な被害を防ぐ対策を講じなければならない。また、無線局を正しく運用し、暗号化や認証システム等を用いて安全性の高い無線ＬＡＮ環境を利用者に提供しなければならない。

4.3.3 ネットワークの監視

ネットワーク責任者は、担当するネットワークを常時監視し、不正アクセ

スの阻止およびトラフィックの状況管理をしなければならない。

4.3.4 ウイルス対策

ネットワーク責任者は、コンピュータウイルス検知・除去を目的とした、ウイルスチェックサーバシステムを導入し、本学ネットワークへの侵入を防ぐ対策を講じなければならない。

4.3.5 外部ネットワークへの接続

システム管理責任者は、本学ネットワークシステム以外の外部ネットワークを利用する場合に本学のネットワークにおけるセキュリティに悪影響を与えてはならない。

4.4 サーバにおけるセキュリティ

4.4.1 認証および暗号化

システム管理責任者は、認証システムにより利用権限を明確にして利用させなければならない。また、個人情報を含む重要なデータがネットワーク上を行き来する場合においては、暗号化等による特段の処置を講じなければならない。

4.4.2 アクセスログ等の管理

システム管理責任者は、システムログやアクセスの記録等、運用に関する記録を一定期間保存しなければならない。また、監査等の実施にあたって記録の提示を求められた場合は、その指示に従わなければならない。

4.4.3 データのバックアップ

システム管理責任者は、サーバ機器に記録されているデータを定期的にバックアップしなければならない。また、保持する情報の性質に応じてバックアップするタイミングを決めておかなければならない。

５．人的な対応

5.1 教育・研修

情報セキュリティ最高責任者は、情報セキュリティに関する啓発や教育を全学的に実施するために必要な措置を講じなければならない。また、利用者は、講習会および研修会を通じて情報セキュリティ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を生じさせないように努めなければならない。

5.2 事故・障害の報告

利用者は、情報セキュリティに関する事故や障害、公開情報の改ざん等を発見した場合には、ネットワーク責任者またはシステム管理責任者に直ちに報告しなければならない。ネットワーク責任者およびシステム管理責任者は、報告のあった内容について、必要な措置を講じなければならない。

ネットワーク責任者は、発生した情報セキュリティ上の事故・障害等に関する記録を一定期間保存し、情報セキュリティ最高責任者に報告するとともに、重大な事故に対しては迅速な再発防止策を講じなければならない。また、利用者に対しては、問題の程度に応じて適切な表現に配慮した通知を行わなければならない。

本学からの不正アクセス等によって学内外に被害を及ぼし、その事実関係の説明を被害者または第三者から求められた場合は、情報セキュリティ最高責任者が関連部署と連携して対応しなければならない。

なお、事故の内容によっては、公的機関に報告することも必要である。さらに、必要に応じて警察のネットワーク犯罪担当部署への相談も検討する。

5.3 措置

システム管理責任者は、情報セキュリティポリシーに違反した利用者に対し、利用資格の停止、取り消し等の措置をとることができる。また、情報セキュリティ最高責任者は、重大な違反に対して、他の学内意思決定組織と連携して必要な措置をとらなければならない。

5.4 システム保守ならびに管理業務の外部委託

システム管理責任者は、システム保守ならびに管理業務を外部委託業者に委託する場合、外部委託業者から下請けとして受託する業者も含めて、外部委託業者との契約において守るべき遵守事項を明確にしなければならない。

６．評価・見直し

6.1 ポリシー運用実態の把握

情報セキュリティ最高責任者は、全学における情報セキュリティポリシーの運用実態について、定期的および必要に応じて調査し、その実態を分析・評価した上で、情報センター運営委員会に報告しなければならない。

6.2 利用者の意見

情報セキュリティ最高責任者は、利用者からポリシー遵守に関する意見を収集し、教育研究上の利便性を著しく損なうことのないよう配慮しなければならない。

6.3 ポリシーの見直し

情報セキュリティ最高責任者は、ポリシー運用実態の把握と利用者の意見等に基づいてポリシーの実効性を評価し、必要な部分を見直して、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しなければならない。

6.4 セキュリティ計画および予算措置

情報セキュリティ最高責任者は、評価・見直しの結果を踏まえ、情報センター運営委員会の審議を経て、情報セキュリティ計画およびそれに対する必要な予算措置を講じなければならない。

6.5 報告義務

情報セキュリティ最高責任者は、必要に応じて他の学内意思決定組織に評価・見直しの結果を報告するものとする。また、その要約を全学の利用者に周知しなければならない。