情報セキュリティ方針
（公益財団法人ハイパーネットワーク社会研究所）

１．目的

公益財団法人ハイパーネットワーク社会研究所は、研究所の情報資産を適切に保護･管理するため、以下の情報セキュリティ方針を策定する。

２．基本用語の定義

この情報セキュリティ方針および関連文書における用語は以下の通り定義する。

2-1 情報セキュリティ

情報の機密性、完全性及び利用の可用性を維持することをいう。

・機密性：認可された者だけが情報にアクセスできるようにすること。
・完全性：保有する情報が正確であり、完全である状態を保持すること。
・可用性：許可された者が必要なときにいつでも情報にアクセスできるようにすること。

2-2 脅威

自然災害、機器障害、悪意のある行為等、損失を発生させる直接の要因のことをいう。

2-3 脆弱性

アプリケーションやシステムの欠陥、設備の欠陥、そのほか脅威を発生しやすくさせる要因、脅威を増加させる要因のことをいう。

2-4 情報セキュリティマネジメント

組織の情報セキュリティ対策を統括的に実施することをいう。

３．情報セキュリティ方針の適用範囲

情報セキュリティ方針の適用範囲は、研究所の情報資産に関連する人的・物理的・環境的リソースも含むものとする。

４．情報セキュリティ方針の適用者

情報セキュリティ方針の適用者は、研究所の情報資産を利用するすべての所員とする。

4-1 所長の責務

所長は、研究所における情報セキュリティマネジメントに関しての最高責任者であり、情報セキュリティ方針への支持・支援を表明し、率先して情報セキュリティマネジメントを推進しなければならない。

4-2 所員の責務
所員には、研究所の情報資産の使用を認めるが、それは、円滑な業務遂行の手段としての使用を認めることであり、私的利用を許可するものではない。所員は、情報資産を扱う上で、信頼を得る研究活動のために、情報セキュリティ方針に同意し、遵守しなければならない。

4-3 外部委託業者への対応
研究所の情報資産に係わる作業を、外部委託業者に依頼する場合には、契約上で遵守するべき情報セキュリティ管理策を明確にする。

５．情報セキュリティポリシーの構成と位置付け
情報セキュリティポリシーは、情報セキュリティ方針と情報セキュリティ対策標準からなる。さらに、対策標準を具体的な手順で記述したものを情報セキュリティ実施手順という。なお、情報セキュリティ対策標準および情報セキュリティ実施手順は、公にすることにより当研究所の運営に重大な支障を及ぼすおそれがあるため非公開とする。

5-1 情報セキュリティ方針
情報セキュリティ方針は、研究所の情報セキュリティマネジメントにおける基本方針を記述したものであり、本文書がこれにあたる。

5-2 情報セキュリティ対策標準
情報セキュリティ対策標準は、情報セキュリティ方針に基づいて、項目毎に遵守すべき事項を記述する。

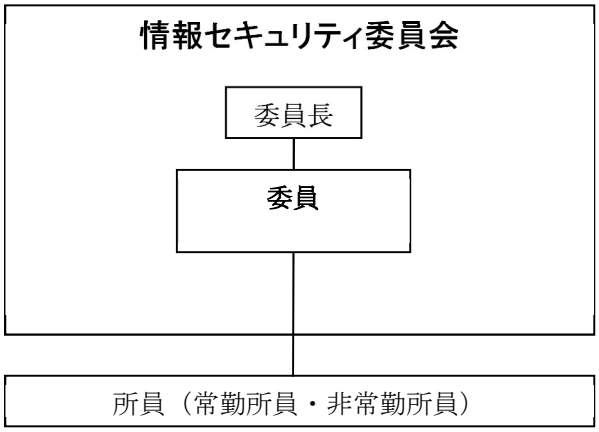
5-3 情報セキュリティ実施手順
情報セキュリティ実施手順は、対策標準で記述された文書をより具体的に手順で示す。

5-4 その他関連法規
情報セキュリティポリシーは、関連法規と照らして違反することの無いようにしなければならない。また、必要に応じて関連規格に遵守した管理策を導入しなければならない。

６．体制
研究所の情報セキュリティマネジメントを遂行する体制を以下の通り定める。

6-1 情報セキュリティ委員会
研究所の情報セキュリティを維持していくために、情報セキュリティ委員会を設け、マネジメント体制を整えるものとする。

6-2 情報セキュリティ委員会の構成
情報セキュリティ委員会の構成は下図の通りとする。



6-3 委員長
委員長は、所長が務める。

6-4 委員
委員は、所員の中から委員長が任命する。

７．情報セキュリティ委員会の役割と責務
情報セキュリティ委員会の主な役割を下記の通り定める。

7-1 情報セキュリティマネジメントの企画及び計画
情報セキュリティ委員会は、研究所における情報セキュリティマネジメントを企画及び計画し、実施しなければならない。

7-2 情報資産の管理方法の策定
情報セキュリティ委員会は、情報資産目録の作成や管理責任者の指名等の情報資産管理や、外部サービスの利用についての取り決め等の策定を行う。

7-3 情報セキュリティ教育の実施
情報セキュリティ委員会は、情報セキュリティに関する継続的かつ定期的な情報セキュリティ教育を行う。

7-4 情報セキュリティポリシーの遵守状況の評価及び改訂
情報セキュリティ委員会は、所員の情報セキュリティポリシー遵守状況を定期的に調査し、情報セキュリティポリシーのレビューを行うこととする。また、所員の情報セキュリ

ティポリシーに対する意見や要望を収集し、その妥当性を評価するとともに必要に応じて内容の改訂を行うこととする。

7-5 情報セキュリティインシデント発生時の対応
セキュリティ委員会は、情報セキュリティポリシーに違反した事項の重要度を評価し、適切な処置を講じることとする。研究所の情報セキュリティが侵害されたと思われる事象が判明した場合は、速やかに対応しなければならない。

８．違反時における罰則
情報セキュリティポリシーの違反者に対する処分は就業規定によるものとする。

９.リスク評価とリスク管理
当法人は、情報セキュリティリスクの評価と管理を行い、リスクを理解し、適切に対処する。

１０.アクセス制御
当法人は、誰がどの情報にアクセスできるかを明確にし、情報の機密性と完全性を保護する。

１１.方針のレビューと更新
本方針は、年に一度、または重要な変更があった場合にレビューされ、必要に応じて更新する。方針の更新は、情報セキュリティ委員会によって承認されるものとする。

改定日　令和６年６月７日
公益財団法人ハイパーネットワーク社会研究所
所長　青木　栄二