

社団法人九州地方計画協会 機密保持基本方針

制 定 : 2006年12月21日

改訂履歴

版数	改訂日	改訂理由、主な内容	作成	確認	承認
1	2006/12/21	初版			

社団法人九州地方計画協会

目 次

第1条 目的	2
第2条 適用範囲	2
第3条 定義	2
第4条 全従業者の責務	3
第5条 外部委託	3
第6条 情報セキュリティ管理体制	3
第7条 情報資産の重要性分類	3
第8条 管理規定	3
第9条 情報セキュリティ対策	3
第10条 情報セキュリティ実施手順	4
第11条 管理規定及び、実施手順の取り扱い	4
第12条 情報セキュリティの点検	4
第13条 評価及び見直しの実施	4
第14条 違反への対応	4
付 則	4

機密保持基本方針

制 定 2006年12月21日

第1条 目的

この基本方針は、高度情報通信ネットワーク社会の到来に伴い増大する情報への脅威に的確に対応するとともに、社団法人九州地方計画協会（以下「協会」という）内機密情報や顧客から預かった情報等、協会が保有する情報資産に対しその重要度に応じて機密性、完全性及び可用性を維持するため、必要な事項を定めることを目的とする。

第2条 適用範囲

本規定が適用される範囲は次の通りとする。

1. 適用場所は、協会事務所の敷地内、現場事務所、詰め所など、主に協会の情報を取り扱うことを主たる目的とする場所とする。
2. この基本方針の適用範囲は、協会全部署に属する全従業員で情報に接する可能性のあるものとする。
3. 適用期間は全従業員の採用時ないし各種契約の成立と同時に適用され、原則として、退職・離職後も協会の保有する情報に関して秘匿しなければならない。そのため、協会は別途定める誓約書を作成し、全従業員から取得する。

第3条 定義

1. 情報資産
 - ・情報システムで取り扱う全ての情報
 - ・紙等の有体物に出力された全ての情報、及び紙等の有体物にて入手した全ての情報
 - ・上記以外の協会が保有する無形の情報
2. 情報セキュリティ
情報資産の重要度に応じて機密性、完全性及び可用性を維持することをいう。
 - ・機密性とは、権限のない者への情報の漏洩を防止することをいう。
 - ・完全性とは、情報の改ざん、破壊による被害を防止することをいう。
 - ・可用性とは、権限のある者に対し、情報の利用を可能にすることをいう。
3. 全従業員
協会の理事長、理事及び、役員を始め、協会全部署に所属する、全職制職務の正職員、出向職員、嘱託業務職員、臨時採用・期間採用・派遣・アルバイト・パートの職員を含むものとする。
4. 情報システム
協会が管理するコンピュータシステム（ハードウェア、ソフトウェア、ネットワーク及びあらゆる可搬記憶媒体）をいう。
5. ネットワーク
協会における組織を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及び記憶媒体で構成され、処理を行う仕組みをいう。
6. 情報資産への脅威
脅威とは、盗難、漏洩、改ざん、破壊、入力・操作ミス等の人的な脅威、故障、誤動作等の情報システムにおける脅威及び地震、火災、水害等の自然の脅威をいう。

7. 区画

協会施設において、作業区画、管理区画に区画を峻別する。

- ・作業区画

全従業員が立入り可能な執務を行う区画をいう。外来者の立入りは規制される。

- ・管理区画

重要な情報資産及び重要な情報システム（ネットワークの基幹機器を含む）の管理並びに運用を行うための区画、ないし施錠可能な保管器そのものをいう。

第4条 全従業員の責務

全従業員は情報資産の取り扱いにあたっては、関係法規の規定及びこの基本方針を遵守しなければならない。

第5条 外部委託

外部事業者との間で委託契約等を締結し、かつ情報処理を行わせる場合には、別途定める「[外注先委託契約等における情報保護管理に関する規定](#)」を遵守させるものとする。

第6条 情報セキュリティ管理体制

協会の情報資産について、機密保持管理上、情報セキュリティ対策を推進・管理するため、[統括情報責任者](#)、[情報管理責任者](#)、[各部署の責任者及び担当者](#)、[システム管理者及び担当者](#)を置く。

第7条 情報資産の重要性分類

情報資産を、その重要度に応じて区分し、当該分類に応じたセキュリティ対策を講じるものとする。

第8条 管理規定

この基本方針に基づき、協会機密にかかる情報セキュリティ対策を実施するにあたっての具体的な基準を統一的に定めるため、「機密保持規定」及び「情報システム運営管理規定」（以下「管理規定」という。）を策定する。

第9条 情報セキュリティ対策

情報資産を、脅威から保護するため、以下の対策を講じる。

1. 機密保持、情報セキュリティ管理について

当協会における情報セキュリティ対策を推進・管理するための体制を確立すると共に、「機密保持基本方針及び機密保持規定、情報システム運営管理規定」（以下『情報セキュリティポリシー』という）の教育や評価・見直し等を含む継続的な管理の仕組みを構築する。

2. 物理的対策について（物理的セキュリティ対策）

情報資産を保管又は設置する施設への不正な立ち入り、情報資産への損傷、妨害等から保護するために物理的な対策を講じる。

3. 人的対策について（人的セキュリティ対策）

全従業員に対して情報セキュリティの重要性を認識させるとともに情報セキュリティの啓発に有効と考えられる研修等の必要な対策を講じる。

4. 技術的対策について（技術的セキュリティ対策）
情報システムを不正アクセス等から保護するため、アクセス制御、ネットワーク管理等の技術的対策を講じる。
5. 運用管理について（運用におけるセキュリティ対策）
情報セキュリティの監視、関係法規及びこの基本方針の遵守等、運用面の対策を講じる。

第10条 情報セキュリティ実施手順

情報セキュリティポリシーに基づき、情報資産ごとに必要に応じて情報セキュリティ実施手順（以下「実施手順」という。）又は事務マニュアル等を作成及び改正するものとする。

第11条 管理規定及び、実施手順の取り扱い

管理規定及び、実施手順は、公にすることにより、情報セキュリティ対策に支障を及ぼすおそれがあるため、公表しない。

第12条 情報セキュリティの点検

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて点検を実施する。

第13条 評価及び見直しの実施

点検の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

第14条 違反への対応

1. 全従業者が、情報セキュリティポリシー等に定める対策に違反した場合は、当協会「就業規則」に規定する懲戒の対象とするほか、情報資産の利用に制限を加えることができる。
2. 情報セキュリティポリシー等に定める「努力規定」については、直ちに罰則を適用するものではない。

付 則

1. この方針は、平成18年12月21日から施行する。
2. この方針を改廃する場合は、協会を代表する者の意見を聞いて行うものとする。