一般財団法人保安通信協会情報セキュリティの基本方針

（制定　令和2年6月29日　協会規程第1号）

1　情報セキュリティの基本方針

(1) 情報セキュリティの基本方針

一般財団法人保安通信協会(以下「本会」という。)において、「一般財団法人保安通信協会定款」に定められた目的及び事業の継続的かつ安定的な実施を実現するためには、適切な情報セキュリティ対策を講じていくことが必要不可欠である。

情報セキュリティの基本は、本会で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり、本会が自らの責任において情報セキュリティ対策を講じていくことが原則となる。

このため、本会においては、情報セキュリティ対策の包括的な規程として、「一般財団法人保安通信協会情報セキュリティポリシー」(以下「セキュリティポリシー」という。)を策定し、本会の情報資産をあらゆる脅威から保護するために必要な情報セキュリティの確保に最大限取り組むこととする。

(2) 適用範囲

ア　本基本方針は本会の事務に従事する役員及び職員（協力会社社員を含む。以下「職員等」という。）に適用する。

イ　本基本方針は、以下の情報に適用する。

（ア）本会の事務に従事する者が職務上使用することを目的として、本会が調達・開発した情報処理若しくは通信の用に供するシステム又は電磁的記録媒体に記録された情報（当該情報システムから書面に出力された情報及び書面から情報システムに入力された情報を含む。）

（イ）その他の情報システム又は電磁的記録媒体に記録された情報（当該情報システムから書面に出力された情報及び書面から情報システムに入力された情報を含む。）であって、職員等が職務上取り扱う情報

（ウ）（ア）・（イ）のほか、本会が調達・開発した情報システムの設計又は運用管理に関する情報

ウ　本基本方針は、イに掲げた情報を取り扱う全ての情報システムに適用する。

(3) 法令等の遵守

情報及び情報システムの取扱いに関しては、本基本方針のほか法令及び基準等（以下「関連法令等」という。）を遵守するものとする。

2 組織・体制の整備

(1) 最高情報セキュリティ責任者及び副最高情報セキュリティ責任者の設置

ア 最高情報セキュリティ責任者の設置

本会における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者1人を置く。

イ 副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、必要に応じて、最高情報セキュリティ責任者を補佐し、本会における情報セキュリティに関する事務を整理する副最高情報セキュリティ責任者1人を置くことができる。

ウ 最高情報セキュリティ責任者の任務

最高情報セキュリティ責任者は、情報セキュリティ対策を着実に進めるために、自ら本会内を統括し、本会全体として計画的に対策が実施されるよう組織・体制を整備し、その活動の推進を図る。

なお、最高情報セキュリティ責任者は、本基本方針に定められた自らの担務を、副最高情報セキュリティ副責任者その他の本基本方針に定める責任者等に担わせることができる。

(2) 情報セキュリティ対策委員会の設置

本会における情報セキュリティ対策を確実に遂行するため、情報セキュリティ対策に関する企画、実施、監査等を審議する「情報セキュリティ対策委員会」を置く。

(3) 情報セキュリティ監査責任者の設置

最高情報セキュリティ責任者の指示に基づき実施する監査に関する事務を統括する情報セキュリティ監査責任者1人を置く。

また、情報セキュリティ監査責任者の下に、情報セキュリティ監査責任者を補佐し、セキュリティ監査に関する事務を整理する情報セキュリティ監査担当者を置くことができる。

(4) 情報セキュリティ管理責任者等の設置

最高情報セキュリティ責任者の指示に基づき実施する情報セキュリティ対策に関する事務を統括する情報セキュリティ管理責任者1人を置く。

また、情報セキュリティ管理責任者の下に、業務の特性等から同質の情報セキュリティ対策の運用が可能な情報システム若しくは組織ごとに、情報セキュリティ管

理責任者を補佐し、各々の情報セキュリティに関する事務を整理する以下の情報セキュリティ管理者等を置く。

ア システムセキュリティ管理者

イ システムセキュリティ維持管理者

ウ 区域情報セキュリティ管理者

エ システム運用管理者

(5) 最高情報セキュリティアドバイザーの設置

情報セキュリティに係る専門的な知識及び経験に基づいて最高情報セキュリティ責任者に助言を行う最高情報セキュリティアドバイザー1人を置く。

(6) 情報セキュリティインシデント対応チーム及び責任者の設置

情報セキュリティインシデント発生時に、迅速かつ的確に対応するため、最高情報セキュリティ責任者の下に、本会の情報セキュリティインシデント対応チーム(以下「 SCA-CSIRT 」(Security Communications Association-Computer Security Incident Response Team)という。)を置き、SCA-CSIRT に関する事務を整理する SCA-CSIRT 責任者1人を置く。

(7) 兼務を禁止する役割

ア 職員等は、情報セキュリティ対策の運用において、以下の役割を兼務できないものとする。

(ア) 承認又は許可(以下「承認等」という。)の申請者と当該承認等を行う者(以下「承認等権限者」という。)

(イ) 監査を受ける者とその監査を実施する者

イ 職員等は、承認等を申請する場合において、自らが承認等権限者であるときその他承認等権限者が承認等の可否の判断をすることが不適切と認められるときは、当該承認等権限者の上司又は適切な者に承認等を申請し、承認等を得るものとする。

3 内部規程の整備

(1) 情報セキュリティ対策基準の整備

最高情報セキュリティ責任者は、情報セキュリティ対策委員会における審議を経て、情報セキュリティ対策基準を定めるものとする。本方針と情報セキュリティ対策基準とを以てセキュリティポリシーに位置づけるものとする。

(2) 情報セキュリティ対策を総合的に推進するための計画の整備

最高情報セキュリティ責任者は、情報セキュリティ対策委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めるものとする。また、対策推進計画には、全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含めるものとする。

（ア）情報セキュリティに関する教養
（イ）情報セキュリティ対策の自己点検
（ウ）情報セキュリティ監査
（エ）情報システムに関する技術的な対策を推進するための取組
（オ）前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

4 職員等の責務

職員等は、情報システム及び本会の事業に関連する情報等を適正に取り扱うものとする。

5 継続的な改善

最高情報セキュリティ責任者は、情報セキュリティの運用、監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、必要に応じて、情報セキュリティ対策委員会の審議を経て、情報セキュリティ対策の継続的な改善に当たるものとする。

附 則

この規程は、令和2年6月29日から施行する。