財団法人e－とくしま推進財団セキュリティポリシーの概要

序章

当財団の情報資産を、内外的な脅威から防御するための指針として、「財団法人e－とくしま推進財団セキュリティポリシー」を策定する。

○セキュリティポリシーの構成

セキュリティポリシーは、基本方針、対策基準、実施手順の3階層の構成とする。基本方針は、他の財団規程と同様の位置づけとし、できるだけ長期的に不変な内容とする。また、策定及び改訂には理事会の議決を要するものとする。

文　書　名	定　　義	策　定　者
(1)情報セキュリティ基本方針	情報資産を適切に保護･管理することを責任者が意思表明したもの（原則公開）	理事会の議決を要する
(2)情報セキュリティ対策基準	基本方針に従い、必要な対策を分野別に規定したもの　（原則非公開）	情報セキュリティ委員会
(3)情報セキュリティ実施手順	対策基準を現場で運用するために、より詳細･具体的に規定したもの（必要に応じて策定）　（原則非公開）	情報セキュリティ委員会

1．目的

当財団が保有する、情報資産を内･外的脅威から防御するために、すべてのネットワーク及び情報システムが高度な安全性を有するとともに、情報資産の機密性、完全性及び可用性を確保･維持するための方針を策定する。

2．基本用語の定義

セキュリティ基本方針における、主な用語について定義する。

3．情報セキュリティポリシーの適用範囲

ポリシーの適用範囲は、当財団の保有する情報資産及び情報資産に接する役員･会員･職員（臨時職員含む）とする。

4．職員等の義務

委託業者を含み、職員等が遵守すべき事項、また、責任について規定。

5．情報セキュリティ管理体制（下表参照）

○管理体制

最高統括情報管理責任者を筆頭とし、当財団のセキュリティポリシーの実施及び管理について、職員等が担う役割を規定する。

○情報セキュリティ委員会

当財団のリスクアセスメント及びリスクマネジメントを実施する機関として、セキュリティ委員会を設置する。委員長には理事長を充て、ポリシーの策定･評価などを実施する。

ポリシーを遵守できない状況が発生した場合、委員会の承認により例外事項とすることができる。また、緊急時（ウイルス対策･不正アクセス対応等）には統括情報責任者を最高責任者として処理を優先し、委員会に事後報告を行うことができる。

管理体制及びセキュリティ委員会の構成

セキュリティ管理体制	セキュリティ委員会	財　団
最高統括情報管理責任者	委員長	理事長
統括情報管理責任者	副委員長	事務局長
情報管理責任者	委員	事務局次長
情報管理者	委員	各担当責任者

6. 情報資産の分類

当財団の保有する情報資産については、その重要性に従って分類し、管理するものとする。(詳細は対策基準「情報資産の分類・管理に関する基準」に規定)

7. 情報資産への脅威

当財団の保有する情報資産の機密性、安全性、可用性を脅かす「脅威」について規定する。

(内外的要因によるもの、災害・事故・故障など)

8. 情報セキュリティ対策

当財団の保有する情報資産を、前述した脅威から防御するための対策について規定する。(詳細は対策基準の各項に規定)

(1)物理的セキュリティ対策

機器、設備、事務所等に関するセキュリティ対策

(2)人的セキュリティ対策

情報へのアクセス、教育、外部委託等に関するセキュリティ対策

(3)技術的セキュリティ対策

サーバ、PC、ネットワークの設置、ウイルス対策等に関するセキュリティ対策

(4)運用におけるセキュリティ対策

システム監視、各サービス(Web、メール等)の利用、危機管理等に関するセキュリティ対策

9. 情報セキュリティ対策基準の策定

基本方針に基づき、必要な対策を分野別に規定したもの。(原則非公開)

10. 情報セキュリティ実施手順の策定

定められた対策を、現場で運用するために、必要がある場合は、より詳細・具体的に定めた実施手順を策定する。(原則非公開)

11. 既存の規定との関連(序章の表参照)

基本方針は、当財団の他の規定と同様の位置づけとする。・・・理事会の議決を要する。

対策基準・実施手順・・・委員会が策定する。

12. 職員等に対する処分

職員等がポリシーに違反した場合の処分を規定(詳細は対策基準「セキュリティ違反に関する基準」に規定)

○損害賠償・・・財団就業規則に基づき処分

○分限及び懲戒に係る処分・・・財団処務規程に基づき処分

13. 情報セキュリティ意識の啓発

最高統括情報管理責任者は、職員等のセキュリティ意識啓発の措置を講じなければならない。（対策基準「セキュリティ教育に関する基準」を参照）

14. 情報セキュリティ監査

情報セキュリティ監査の定期的な実施を規定（詳細は対策基準「監査に関する基準」に規定）

15. 評価及び真直しの実施

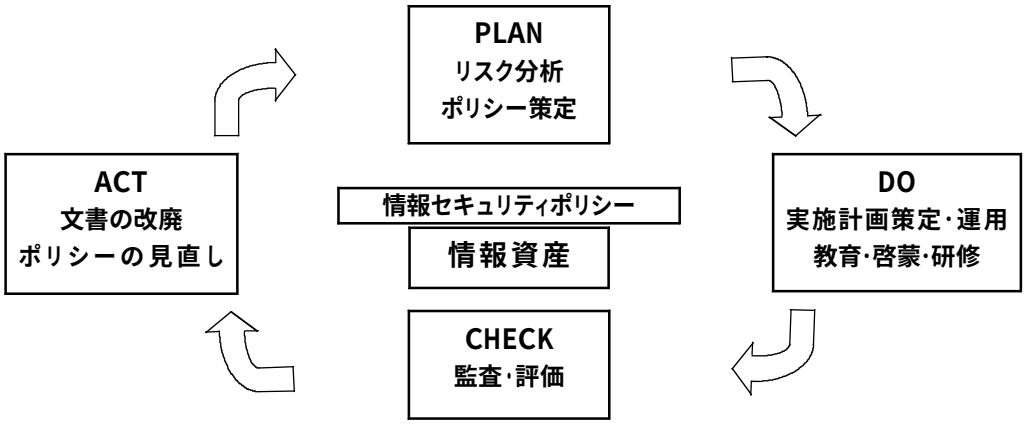
セキュリティ監査の結果等により見直しを行う。

16. 理事会への報告

重要情報の理事会への報告を規定（ポリシーの改定、セキュリティ事故・問題等）

17. 情報セキュリティマネジメント

PDCAサイクル（Plan：計画・Do：実施・実行・Check：点検・評価・Act：処置・改善）に基づき、セキュリティレベルのマネジメントを実施することを規定。（下図参照）



18. 情報セキュリティ侵害時の対応

セキュリティ侵害時の対応について規定（詳細は対策基準「危機管理における対策基準」に規定）

※. 参考文献

「情報セキュリティポリシーサンプル（0.92a版）」
NPO日本ネットワークセキュリティ協会（JNSA）編