

# 山梨県情報セキュリティ基本方針

平成15年 6月12日 制定  
平成17年11月 9日 一部改正  
平成19年 6月 1日 一部改正

## (目的)

第1 この基本方針は、県が保有する情報資産を様々な脅威から防御し、機密性、完全性及び可用性を維持するため、県が行う情報セキュリティに関する対策の統一かつ基本的事項を定めることを目的とする。

## (対象範囲)

第2 この基本方針が対象とする県機関の範囲は、知事部局、企業局、教育委員会事務局、議会事務局、人事委員会事務局、監査委員事務局、労働委員会事務局、選挙管理委員会事務局及び警察本部とする。なお、警察本部については、知事部局が管理運用する情報システムを利用する部署のみを対象とする。

## (定義)

第3 基本方針の用語の意義は、それぞれ次に定めるところによる。

### (1) ネットワーク

電子計算機を相互に接続する通信網及び当該通信網を構成する機器をいう。

### (2) 情報システム

電子計算機及び記録媒体で構成され、電子情報処理を行う仕組みをいう。

### (3) 情報資産

ア ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体

イ ネットワーク及び情報システムで取り扱う情報(これを印刷した文書を含む。)

ウ ネットワーク及び情報システムに関連する文書

### (4) 情報セキュリティ

情報資産について、次に掲げる状態を維持することをいう。

ア 機密性 情報資産が正当な使用者に対してのみ、適切な手段で利用される状態

イ 完全性 情報資産が破壊、改ざん又は消去されていない状態

ウ 可用性 情報資産が必要とされているときに、正当な使用者が適切な手段で使用できる状態

### (5) 不正アクセス

不正アクセス行為の禁止等に関する法律(平成11年法律第128号)第3条第2項で定義している行為をいう。

## (職員の遵守義務)

第4 職員(再任用職員、非常勤嘱託職員及び臨時職員を含む。以下同じ。)は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たってこの基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守しなけ

ればならない。

(情報資産への脅威)

第5 情報資産に対して想定される脅威は、次のとおりとする。

- (1) 故意又は過失による情報資産の持出、盗聴、改ざん、消去、盗難、漏えい及び破損
- (2) 地震、落雷、火災等の災害、事故及び故障による業務及び行政サービスの停止

(情報セキュリティ対策)

第6 情報資産を、前項の脅威から保護するため、次の情報セキュリティ対策を講じるものとする。

(1) 人的情報セキュリティ対策

情報セキュリティに関する権限や責任及び遵守すべき事項を定め、職員等に対する周知及び徹底を図るとともに、十分な教育啓発が行われるよう必要な人的対策を講ずる。

(2) 物理的情報セキュリティ対策

情報資産を有する施設への不正な立入り、損傷、盗難等の事故及び災害から情報資産を保護するための物理的な対策を講ずる。

(3) 技術的情報セキュリティ対策

情報資産を不正アクセス等やウイルスから保護するため、情報資産へのアクセス制御、ウイルス対策等の技術的対策を講ずる。

(4) 運用による情報セキュリティ対策

情報資産の管理、セキュリティ対策の遵守状況の確認、緊急事態発生時の危機管理対策等、セキュリティ対策の運用面の対策を講ずる。

(情報セキュリティ対策基準の策定)

第7 この基本方針に基づき、情報セキュリティ対策を具体的に実施するにあたっての遵守すべき事項や、判断等の基本的な基準として、情報セキュリティ対策基準(以下「対策基準」という。)を策定するものとする。

(情報セキュリティ実施手順の策定)

第8 基本方針及び対策基準に基づき、情報セキュリティ対策を実施するため、個々の情報システムについて、具体的な実施手順を明記した情報セキュリティ実施手順(以下「実施手順」という。)を策定するものとする。実施手順は、公開することにより県の行政運営に支障を及ぼす可能性がある情報であることから非公開とする。

(監査及び自己点検)

第9 情報セキュリティが確保されていることを確認するために、定期的又は必要に応じて情報セキュリティ監査及び自己点検を行う。

(評価及び見直し)

第10 情報セキュリティの検証の結果等に基づき、情報セキュリティの状況を評価するとともに、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、必要に応じてこの基本方針、対策基準及び実施手順の見直しを実施する。