

情報セキュリティポリシーについて

1 情報セキュリティと個人情報保護

情報セキュリティの問題は、情報がコンピュータにより処理された時から始まっています。そして、近年の情報化の進展に伴い、行政情報をはじめ、各種個人情報が電子化され、大きな利便性がもたらされる一方で、大量の情報が漏洩したり、情報が簡単に改ざんされたりする脅威が増大しています。

こうした脅威から区の情報資産を守るために、情報セキュリティ対策への取り組みの徹底が必要です。

「情報セキュリティ」とは、重要な「情報資産」に関して、機密を守り（情報の機密性）、誤った使用や改ざんを防ぎ（情報の完全性）、許可された人が必要なときに安全確実に利用できる（情報の可用性）ようにしておくことです。

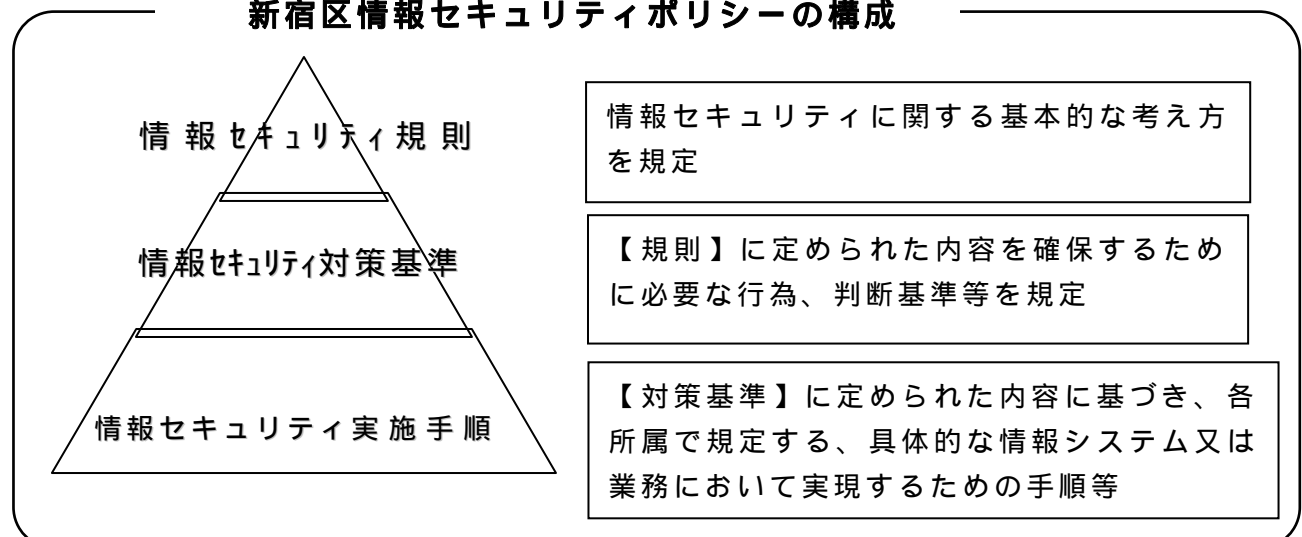
「情報資産」とは、情報システム及びネットワークで取り扱う個人情報を含むすべての情報、及び情報システム及びネットワークの開発、運用等に係わるすべての情報のことです。

2 新宿区情報セキュリティポリシー

区では、平成 15 年 8 月 25 日に「新宿区情報セキュリティポリシー」を制定しました。

情報セキュリティポリシーとは、区の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめ文書化したものの総称です。情報の安全性の確保と行政の安定的運営が目的です。

新宿区情報セキュリティポリシーの構成



3 情報セキュリティポリシーを維持するための体制

情報セキュリティポリシー全体を管理する体制としては、情報資産や情報セキュリティに関する最終決定権限及び責任を有する情報化統括管理者（CIOと称します。）に副区長を任命し、その下にネットワーク管理者（総合政策部長）を置いています。さらに、各所属における情報資産については、統括情報セキュリティ責任者（部長級）、情報セキュリティ責任者（課長級）を定め、管理や責任の所在を明らかにしています。

4 情報セキュリティ対策

情報セキュリティポリシーでは、どのような情報資産をどのような脅威からどのように守るのか、についての基本的な考え方を規定しています。

（1）情報資産に対する物理的な対策

- ・情報システムを設置する施設の入退出管理
- ・自然災害等に備えた施設面の対策等

（2）情報資産に対する技術的な対策

- ・定期的な情報資産のバックアップ
- ・適切な利用者権限の登録（利用者識別＝ID、パスワードの設定）
- ・操作記録の保存
- ・許可なき情報資産の持ち出し禁止
- ・機器やネットワークに対する不正接続の防止
- ・適切なネットワーク経路の制御（情報の暗号化等）
- ・情報資産を記録した機器等廃棄の際には情報資産の完全消去
- ・コンピュータウイルス対策
- ・外部からの情報システムへの不正侵入の防止（ファイアウォール等）

（3）情報資産に対する人的な対策

- ・情報セキュリティポリシーの周知徹底
- ・管理や役割に応じた情報セキュリティに関する研修