和歌山県内市町村のセキュリティポリシー策定・運用への取り組み

特定非営利活動法人　情報セキュリティ研究所　山地　真嗣
yamaji@riis.or.jp
キーワード：情報セキュリティ，セキュリティポリシー，セキュリティ監査，セキュリティ教育

１．はじめに

情報セキュリティの必要性が叫ばれる中、和歌山県内の市町村は自主的にセキュリティ対策協議会を設立し、共同でセキュリティポリシー策定、実施手順書の作成、職員研修、内部監査人の養成および内部監査などの活動を行っている。ＮＰＯ　情報セキュリティ研究所は、自治体セキュリティ対策協議会の活動を支援する立場にある。

自治体と同じく､情報セキュリティが要求される学校においても､これらの活動は参考になるものと思われるので、自治体セキュリティ対策協議会の活動を紹介する。

２．活動の内容

２．１　背景

住民から個人情報を含むさまざまな情報を預託され、それらを基に住民サービスを行う自治体では、情報セキュリティ対策は必須の事項である。

しかし、実態は業務の効率化が優先され、情報セキュリティ対策は二の次であることが多い。また、もぐらたたき的な情報セキュリティ対策をとることも多い。

一方で、増加する情報セキュリティ事件により、自治体に対する住民の目は厳しさを増しつつある。

情報セキュリティ対策予算も乏しく、定期的な人事異動のため情報セキュリティの専門家を育成することもままならない、地方自治体にとっては非常に悩ましい状況にある。

また、LGWAN やその他のネットワークで接続され、相互に情報の交換を行う自治体間においては、ひとつの自治体でのセキュリティ事件・事故が他の自治体にも波及しかねない。すべての自治体が同等のセキュリティレベルにあることが要求される。

２．２　自治体セキュリティ対策協議会のメリット

このような状況を打開するため、和歌山県内の市町村は自主的にセキュリティ対策協議会を設立し、共同で情報セキュリティ対策にとりくむことにした。共同で行うことで次のようなメリットが考えられた。

（１）　相互に関係のある自治体間のセキュリティレベルを同一に保てること。
（２）　対策の検討費用や教育費用を自治体数で分担することができ、少ない予算で効率的に行えること。
（３）　横のつながりが広がり、各自治体が持つノウハウを共用することができること。

２．３　情報セキュリティの維持・運用のために何をするのか

図１は、情報セキュリティを維持・運用するためにどのようなことをするのかをまとめたものである。情報セキュリティを維持・運用することは、情報セキュリティポリシーを作ればそれで終わりではない。維持・運用するということは、マネジメントするということでもある。

すなわち、計画を立て（Plan)、それを実施し（Do)、うまくそれが機能しているのかをチェックし（Check)、是正を行う（Action)、必要なら計画の見直しも行うという、PDCA をまわしながら、よりよい状態にしてゆくことである。

図１に示す流れに沿って、協議会では平成 15 年から、次のような活動を行ってきた。

（１）　情報セキュリティポリシーの策定
（２）　情報セキュリティ実施手順書の作成
（３）　全職員および管理職に対する情報セキュリティ教育
（４）　内部監査人の養成および内部監査

２．４　情報セキュリティポリシー策定時のポイント

情報セキュリティポリシー（情報セキュリティ方針、情報セキュリティ対策基準）の策定においては、次のような点がポイントとなる。

（１）トップがきちんと、情報セキュリティの位置づけを明確にし、必要な支援をすること。
（２）策定にはすべての組織の代表が関わり、具体的な対策基準などを自らが検討すること。
（３）出来上がったものは、きちんと周知すること。

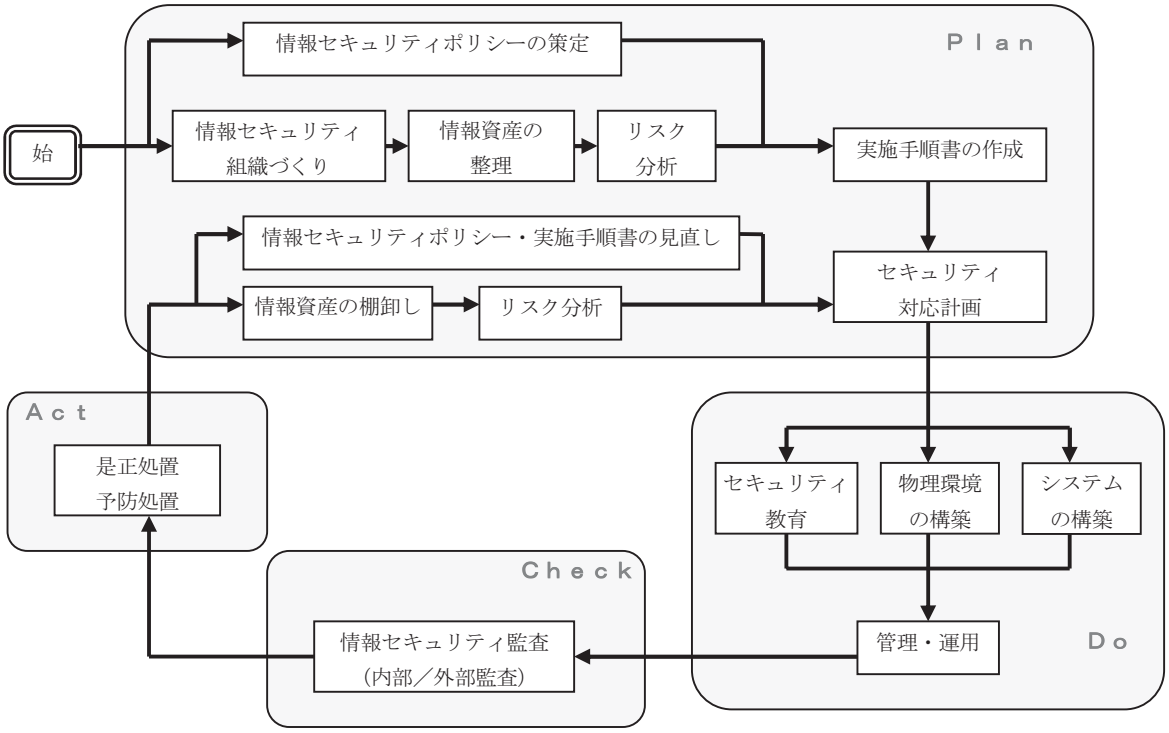

図１ 情報セキュリティポリシーの策定から維持・運用（マネジメント）の流れ

２．５　情報セキュリティポリシー実施手順書作成時のポイント

情報セキュリティ実施手順書の作成では、次のような点がポイントとなる。

（１）情報の取扱いの現状を把握し、実態に沿った対策を検討すること。

（２）現在の状況からすぐに実施・遵守できなくても、いつまでにするという計画を立てること。

２．６　情報セキュリティ教育のポイント

情報セキュリティ教育では、次のような点がポイントとなる。

（１） 組織を構成するすべての人に教育を行うこと。

（２） 継続して行うこと。

２．７　情報セキュリティ内部監査人の養成および内部監査のポイント

内部監査人の養成および内部監査の実施では、次のような点がポイントとなる。

（１） 監査の位置づけを明確に、内部監査人の責任と権限を明確にすること。

（２） 内部監査の指摘事項に対して、いつまでに是正を行うかを明確にすること。

３．　最後に

個人情報保護法が完全施行され、個人情報の取り扱い対する世の中の目は、厳しさを増している。

平成 17 年 12 月には、情報セキュリティに関する政府統一基準が策定された。この基準に従って、各省庁、自治体、独立行政法人などの情報セキュリティの見直しが始まっている。

単独では難しいことも、多数の組織が集まり知恵を出し合うことで解決できることがある。学校関係でも同じく、学校どうしが協力し合って、情報セキュリティレベルを高めていっていただければと思う。

以上