「「第２次情報セキュリティ基本計画」（仮称）に係る検討の視点（例）」に関する意見

2008/2/14
神奈川県藤沢市

資料５

１．基本認識

○現在の社会環境とITが果たす役割について

◇「個」の利用の拡大

情報伝達速度の高速化と伝達量の拡大があるが、官民等の組織的利用だけでなく「個」の利用拡大の流れがある。

特に、ブログや携帯メールなどITのコミュニケーションの手段としての役割に注目する必要があり、旧来の衰退した地縁・血縁に替わり、急速に「電縁」（ネットワーク上の縁）が強まり、新しい価値観や文化の創造が図られてきている。

このため、情報セキュリティとして取り組むべき範囲については、「個」及び「個」が形成する地域社会といった地域コミュニティや、ネットワークコミュニティも考慮する必要がある。

○情報セキュリティ政策に関する現状認識と評価について

◇地方公共団体の立ち後れ

「情報セキュリティ基本計画」が策定されたことにより、政府機関の取組は進みつつある。地方公共団体においてもガイドライン（「地方公共団体における情報セキュリティポリシーに関するガイドライン」総務省）に基づく情報セキュリティポリシーの策定が進むなど、一定の進展が図られた。

しかし、地方公共団体における情報セキュリティレベルには非常に大きな格差が存在し、「情報セキュリティ基本計画」そのものもまだ浸透しているとは思えない。

このため、地方公共団体の実態を把握するとともに、この底上げに重点的に取り組む必要がある。

◇脅威の認識と不安の増幅

ITが国民全体、特に高齢者層に拡大し、かつ「個」の利用が急速に拡大しているが、IT利用に関する脅威の認識が高まるにしたがい、逆に不安を増幅している面もある。

このため、IT利用における利便性及びその脅威とともに、インシデント発生時の対応手段について、国民全体に浸透させる等の不安を除去することが重要である。

また、犯罪を犯している意識の欠如が見られ、ITを利用した犯罪に対する法整備が急務と思われる。

２．総論

○情報セキュリティ政策の理念について

◇受動的から能動的な取組へ

情報セキュリティの対策は、ほとんどが受身の対策として実施されており、対症療法の域を出ていないが、自らがリスクを洗い出し、評価し、対策を立て、実施し、見直していくことが重要で、受動的な取組から能動的な取組への転換が必要である。

このため、情報セキュリティ対策を各主体の責務とするとともに、インセンティブの与え方や持ち方をどうしたら良いかの検討も必要である。

◇意識改革と社会風土

意識改革は必須であり、現在の社会風土を一新する必要がある。そのためには、事象、弱点、インシデント報告の重要性を強調し、さらに、問題発生時には人が悪いのではなく、組織が悪いという風土を定着させる必要がある。

しかし、日本の社会風土の中で、社会的な合意が形成され、定着するような改革は可能であろうか。

◇性善説と性悪説から環境説へ

セキュリティは必ず「性善説」か「性悪説」かの決定論的な議論となり、「どうすれば良いのか」の建設的・生産的な議論に結びつきにくい傾向がある。

このため、「どのような環境であれば情報セキュリティを守る気を起こさせることができるか」という観点が重要で、この「環境説」を採ることにより、具体的な政策をめぐる議論の土壌にあげやすくなる。

〇第2次基本計画の枠組みについて

◇対策実施領域としての地方公共団体の位置づけと扱い

大中小、規模も環境も異なる約1800の地方公共団体は住民や地域に密着して様々な業務を行い、1億2700万人超の個人情報等の情報を預かり、管理している。そして、これらの情報資産価値や脅威はほぼ同様であるが、脆弱性が大きく異なっており、情報セキュリティレベルに非常に大きな格差が存在する。

このため、各地方公共団体の情報セキュリティ対策に「差」があってはならず、取り扱いも含め全国均一な対応が必要で、独立して取り扱うべき重要な領域ではないだろうか。

◇コミュニティやNPOの視点

ITの利活用には、コミュニティや文化に関する視点を加えるべきであり、地域コミュニティやNPO等を情報セキュリティの普及啓発等の担い手と考える発想、支援される対象から推進する主体と捉える発想も必要である。

また、官や市場原理、技術だけでは解決できない課題を、コミュニティで解決するような発想も必要であり、公助、自助に加え、共助の考え方も必要である。

3. 各論

○政府機関・地方公共団体における情報セキュリティ政策について

◇地方公共団体の実態把握

現行の基本計画は政府機関により重点が置かれているが、次期基本計画では地方公共団体の実態をより捉え、進化した計画とする必要がある。

このため、各地方公共団体の情報セキュリティレベルをできるだけ客観的に把握できるように工夫するとともに、情報セキュリティ対策に決定的な影響のあるトップや職員の意識レベルを把握する等、具体的な阻害要因の調査が必要である。（なぜ進まないか）

また、ほとんどの地方公共団体は、既に情報セキュリティポリシーの基本方針や対策基準は策定したことになっているが、PDCAサイクルを毎年確実に実施している団体は、非常に少ないと推測される。さらに、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成18年9月版）」でも実施手順までは定めていないことから、実施手順は未整備となっていると推測される。

このため、情報資産台帳やリスク分析、規程類の見直しをしているか、教育研修や訓練の実態、セキュリティ監査の内容、監査結果の改善結果などを定期的に調査し実態を把握する必要がある。（どこまで進んでいるのか）

市町村の情報セキュリティポリシー策定率と情報セキュリティ研修実施率

市町村　n=1843	H15	H16	H17	H18
個人情報保護条例制定率	73.6%	82.1%	98.0%	100.0%
情報セキュリティポリシー策定率	29.5%	74.4%	92.5%	96.2%
情報セキュリティ研修実施率	21.9%	40.5%	51.5%	61.2%
情報セキュリティ監査実施率	8.9%	11.8%	20.8%	29.1%

平成18年度　地方自治コンピュータ総覧より

◇地方公共団体の成熟度による目標管理

各地方公共団体の情報セキュリティレベルは大きな格差があるが、レベルアップに対するポテンシャルも阻害要因も一律ではない。このため、現状（成熟度）を把握するとともに、段階的な目標を定めて段階的にレベルアップすることが有効と考えられる。

現状把握や目標設定、段階的レベルアップの計画や実施が求められるが、成熟度の判定基準とそれにあわせた目標設定方法のガイドライン作りが必要である。

◇地方公共団体の情報セキュリティ推進要件

情報セキュリティの推進要件は、地方公共団体の規模や地理的環境だけでなく、トップの意識に大きく依存する。また、情報セキュリティ部門の意欲も大きな要素となる。

このため、トップの意識啓発をどのように図っていくかが重要な課題で、全国知事会、市長会、町村会等組織の役割が期待される。

また、組織的に明確な責任体制の構築も必要で、CISOを設置するのもその１つであり、情報セキュリティ部門の明確な権限と位置づけが必要となる。

さらに、首長の責任を明確にするため、情報セキュリティポリシーの条例化も有効ではないか。

◇地方公共団体の課題と解決手法

情報セキュリティポリシーはPDCAサイクルを毎年確実に実施するかや、組織への浸透度が問題となる。

このため、情報資産台帳、リスク分析、規程類の見直し、教育研修の実施、情報セキュリティ監査や緊急時訓練の実施、監査結果等の改善への反映等を計画的に実施することや、実施手順を豊富にそろえること、職員啓発の工夫が必要である。

特に、情報セキュリティポリシーの根幹となるのはリスク分析で、様々なレベルにある地方公共団体には、分かり易いガイドラインや、マニュアルが必要となる。

また、近年の中越沖地震等災害の発生を考えると、大災害発生等に対応する業務継続計画についても、実効性のあるガイドラインやマニュアルが不可欠である。

◇地方公共団体の責任範囲

地方公共団体は様々な情報セキュリティ対策を実施するだけでなく、新たな脅威にも対応する必要があり、さらに、住民や組織内にリスク受容の理解を求める必要がある。

このため、ISMSはリスクをコントロールする1つの手法であるが、どこまで対策を実施すれば良いのか、免責となるかは不明確であり、何らかの指標が必要である。

また、保証型の情報セキュリティ監査、情報セキュリティ保険の創設なども検討する必要がある。

◇地方公共団体の外部委託と地元企業育成

地方公共団体の外部委託は増加しており、委託先からの情報漏えいは大きな問題で、この防止対策が必要である。このため、外部委託事業者の情報セキュリティ対策実施状況の確認や、リスクアセスメント実施後に契約し、契約後に実地検査等による確認を行うことが必要となが、このような取組は多くの地方公共団体にとって大きな負担で実現性が薄い。また、ITゼネコン等の再委託問題や地元ベンダー育成という大きな課題もあり、これらの点も考慮した委託管理のガイドラインが必要である。

◇小規模な地方公共団体の対策

首長の意識や担当部門の意欲が不可欠であるが、まずは人材の育成が必要である。

（財）地方自治情報センターの講師派遣事業やネットワーク機器等の遠隔診断を利用するなど、外部支援機関の利用も有効である。

また、情報システムの共同化やASP、SaaSなどとともに、人材の共同利用、相互利用も検討の必要がある。

◇地域住民の情報セキュリティ対策

地方公共団体は住民の情報セキュリティ対策にも取り組む必要がある。この際NPOやボランティアグループとの協働が有効である。