

情報セキュリティガバナンスに関する調査・研究

本開発・研究事業は、平成22年度自転車等機械工業補振興助事業により実施した事業です。

1. 事業概要及び目的

情報システムが高度化・複雑化するにつれて、民間企業のみならず自治体においても、個人情報保護や情報セキュリティの取組みに関して強い関心が求められており、情報セキュリティガバナンスの在り方が重要な位置づけになっている。また、昨今では、自治体が相互にネットワークにより接続されたり、クラウドコンピューティングによる共通の情報システムの利用、自治体間での情報の提供や利活用など新たな取組みが進んでいる。

そのような状況において、一部の情報セキュリティの脆弱性が、全体の情報セキュリティレベルを下げてしまうことになり、全体での情報セキュリティレベルの底上げを図るためにも、情報セキュリティガバナンスが重要となっている。

そこで、情報通信技術の発展、普及、環境の変化等に対応した情報セキュリティ分野における課題にたいして、以下の2つの観点で調査研究を実施した。

- ①クラウドコンピューティング等の新サービス時代の共通情報セキュリティ基準に関する調査研究
- ②情報セキュリティガバメントのための管理システムの維持管理・運用に関する調査研究

2. 事業の実施内容

全国の自治体や自治体から委託を受けるサービス事業者が住民個人情報を扱う場合に“すぐにそのまま使える”ことを目指した、クラウドコンピューティング利用をも視野に入れた情報システム調達のためのセキュリティ標準仕様案と、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」との整合性を図った新たな情報セキュリティ対策基準案の策定を試みた。現状の課題を探るためにアンケート調査とインタビュー調査により実態調査を行った。

情報セキュリティマネジメントシステム（以下、ISMS とする）は、情報セキュリティの第三者認証制度として、国内でも急速な発展を遂げており、現在（2010年8月）既に約3,600事業所がISMS 第三者認証を取得してい

る。一方、ISMS 第三者認証制度について、課題が明らかになってきた。

- ① 第三者認証を取得したが、当初の想定した実効性を維持・向上できていない。
- ② 取引先企業や親会社から認証取得を迫られ、取得を目的にしたため、十分な体制構築ができずに、苦勞している。
- ③ ISMS 第三者認証制度の根幹にある、「監査」概念に対する理解不足が多くの関係者にある。特に業務監査等の概念は必ずしも十分に理解されていない。

認証取得事業所での教育方法等にも課題があると考え、教育・訓練に焦点を当て、課題の抽出を行い、情報セキュリティ教育のあり方等について調査研究した。現状の課題を探るためにアンケート調査とインタビュー調査により実態調査を行った。

3. 本事業実施による成果

住民個人情報を取扱う情報システムと組織に求められる具体的な情報セキュリティ対策基準の適用課題のなかでも現時点でいちばん優先度が高く、まず新たに導入するシステムやサービスから最低限のセキュリティレベルを確保することを実現させるために、クラウドコンピューティングサービスの調達を含めた「情報システム調達のためのセキュリティ標準仕様」を整備することが有効であり、情報セキュリティ要件は自治体個々で決めるものではなく全国統一であること、情報システムの調達時のセキュリティ要件の指標となるものが必要であることが確認できた。作成した情報システム調達のためのセキュリティ標準仕様案が参考として利用できるツールと成り得、今後増加が予想される ASP サービス利用者のみならず、サービス提供者が整備すべきレベルについての重要な資料になると期待できる。管理システムの維持管理の調査研究では、監査概念（リスクマネジメント主体の考え）についての改善、コンサルの有効利用及び質向上のための評価制度の必要性などの課題が抽出できた。

4. 本事業の成果の活用状況

今回作成した調達対象区分は「情報システムに係る政府調達の基本指針」実務手引書（2007年7月1日総務省行政管理局）」における情報システムの構成例をモデルにして分類しているが、調達対象区分の細分化、特に個別アプリケーションの部分をもう少し具体的なアプリケーション単位に分類しないと対象となるセキュリティ要件の絞り込みができないという課題が残っている。また、調達区分毎の要件抽出を容易にするツール化により、調達区分

を選択すれば、必要となる要件が自動抽出されリストされ、セキュリティ要件の決定をより効率的に実施できるようにすることが必要である。

今回の調査研究で明らかになった今後の課題を踏まえ、情報セキュリティ実装基準の具体化、対応基準の監査ガイドラインの整備、対応基準の有効性確認、「住民個人情報を取扱う情報システム調達のためのセキュリティ標準仕様（案）」の有効性の確認などに向けての対応を推進していく。成果の活用イメージを以下の図に示す。

