第109回月例研究会報告

1. テーマ 「地方公共団体における情報セキュリティ監査について」
2. 日時 2004年12月21日（火） 18時30分～20時30分
3. 場所 中央大学 駿河台記念館 520号会議室
4. 講師 総務省 自治行政局地域情報政策室 係長 高島 史郎 氏

（報告者：No. 898 竹下和孝）

はじめに

今回はじめて総務省から、しかも情報政策推進を担当される方に、直接話を伺う機会をいただきました。

年末の多忙な時期に加え、来年度予算案の調整の重要な時期と重なってしまいましたが、総務省高島様には時間調整だけでなく多大なご協力を頂いて、活発な質疑をおこないました。参加者は85名。

講演概要

１．地方公共団体における情報セキュリティ対策

小学生中学生の頃からネットに親しんだ者が、自治体のサービスの利用者としてだけでなく職員としても自治体活動にもかかわってくる時代になってきたという背景から、より安心安全なサービスを提供するためにも電子自治体への取り組みを急いでいます。

電子自治体を実現するためには、その全国的な共通基盤として、ネットワークと認証基盤を整備する必要があります。具体的には、LGWANという総合行政ネットワークと住民基本台帳ネットワークシステム、認証基盤としてLGPKIという組織認証基盤、公的認証サービスが挙げられます。地方公共団体でも、これらの全国の共通基盤の整備が進み、情報セキュリティ対策への取り組みが進んでいます。

平成15年度に情報セキュリティポリシを策定し、一部の自治体ではありますが平成１６年度には情報セキュリティ監査も開始されています。

平成15年末にまとめた「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書」の中の「地方公共団体情報セキュリティ管理基準」、「地方公共団体情報セキュリティ監査実施手順」及び「セルフチェックリスト」は、「地方公共団体情報セキュリティ監査ガイドライン」として全国の自治体に通知しています。

このように都道府県、及び市区町村では情報セキュリティ監査が開始されております。このため、総務省では、セルフチェック（自己点検）及び情報セキュリティ監査の実施について積極的に指導するなど、地方公共団体における情報セキュリティ監査を促進しています。

２．各団体におけるアプリケーション整備

地方自治体が電子自治体推進を進めるのは、少子高齢化、循環型社会構築、地域経済活性化などへの対応の必要性に迫られてのことです。しかしながら、施策はリソースを選別し選択と集中により対応していかざるを得ないのは、企業だけではありません。従って、地方行政にＩＣＴを積極的に活用して業務改革を進める必然性があるわけです。

自治体は予算を持っていないという話を聞きますが、必要な場所にはちゃんと鍵をかけているわけで、情報セキュリティの予算確保も同じだと考えます。情報セキュリティ監査の実施状況に関しては、「ガイドライン」公表の時点が既に地方公共団体にとって平成16年度予算案をセットした後だったこともあり、本格的な実施は平成17年度からである。したがって、H15.12の指示時点では、県や政令指定都市のように補正予算で実施できる自治体を除くと、H16年度の予算策定に間に合わなかったところが多いので、H17年度での実施に期待しているところです。

３．情報セキュリティ・個人情報保護対策

H15年に内閣府が実施した個人情報保護に関する世論調査では、個人情報の利用に関したプライバシー侵害が増えたという意見が62%あり、今後もコンピュータを利用したプライバシー侵害が多くなるだ

ろうという心配が82%にも達している。行政機関や民間事業者による個人情報の間違った処理を心配する者が58%、地方公共団体が扱う個人情報を保護するための条例制定を望む者が52%もあります。

これらは、個人情報保護と情報セキュリティ対策の重要性を裏付けるもので、地方自治体は更に十分な保護対策を講じることが求めている、と理解しています。

情報システムの安全性・信頼性の確保と個人情報の保護は、電子自治体構築の基盤となるものであり、住民の安心感・信頼性を確保するための前提となるものです。

４．情報セキュリティ対策

情報セキュリティ対策に対する体制整備として、次の２点に注力してきました。

①ＣＩＯの任命（管理体制の整備）

②情報セキュリティポリシの策定

これらの成果として、庁内はもとより、都道府県や市町村でもＣＩＯが任命され、それぞれのセキュリティポリシが制定されました。

都道府県では、主として副知事がＣＩＯを勤め、また市町村では助役が任命されています。これらは、値自体の行政全般を熟知していて全体的ににらみを利かせながら推進していくために、適切な人選だと判断しています。しかし、H16.4時点の調査では、まだ半数の自治体では、ＣＩＯが任命されていません。情報セキュリティポリシの策定状況は、H16.10時点で、都道府県は100%達成、市町村も80%に到達しておりますが、H17.4以降には、実施できていない市町村は公表するなどして整備を加速化させたいと考えています。情報セキュリティは、市町村の合併とは別の課題ですので、合併が完了するまで待つという訳にはいかないと考えます。また市区町村によって地域間のバラツキがあることも指摘されています。

５．地方公共団体の情報セキュリティ監査

H16.4時点での調査では、情報セキュリティ監査を実施している都道府県は17団体で36%、28団体が検討中との結果である。市町村では、370団体が実施済み（11%）、昨年度よりはアップしているが、まだ低調で検討中が1503団体（48%）、未実施が1250団体（40%）である。個人情報保護といっても、民間企業とは内容が異なり、法令に基づき保有しているもので、それが各種証明の基礎データになることから、情報資産の種類や機密の内容も違う。情報セキュリティ対策としての情報セキュリティ監査は、法律で義務付けられたものではないので、強制するわけには行かず、自治体の判断と財政を考慮した政策の優先度に委ねられます。

公共団体が所有する資産に対する情報セキュリティ監査は、行財政監査とは別であり、地方自治法に基づく監査制度とは現時点では分けて考えている。

次に、ＬＧＷＡＮ（総合行政ネットワーク）、住民基本台帳ネットワークシステム、公的個人認証サービス制度など、公共団体とは別の管理者による個別システムの監査が行なわれている。

さらに経済産業省の情報セキュリティ監査制度は、これらとも異なる制度です。

６．地方公共団体の情報セキュリティ管理基準

地方公共団体の情報セキュリティ管理基準の考え方（別紙１）、同管理基準の概要（別紙２、別紙３）を参照してください。これらを普及促進していくために、次の施策（別紙４）を進めているところです。

１）情報セキュリティ監査に関する基準類の管理当のための体制整備
２）地方公共団体に対する情報提供および相談のための体制の整備
３）地方公共団体の共同による情報セキュリティ監査の実施
（地方には、専門経験と知識を持った監査人がいないことへの対応）
４）情報セキュリティ監査に対する財政支援（情報セキュリティ支援フォーラムへの参加促進）
５）地方公共団体における教育研修

別紙１　地方公共団体情報セキュリティ管理基準の概要１（P18）
別紙２　地方公共団体情報セキュリティ管理基準の概要２（P19）
別紙３　地方公共団体情報セキュリティ管理基準の概要３（P20）
別紙４　地方公共団体における情報セキュリティ監査の普及促進策（P21）

情報セキュリティについては、このように安全確保の必然性から具体的な施策へと結びついてきましたが、システム監査については、まだまだこれからです。　システム監査人の皆さんのご理解と、今後のご協力をお願いします。

７．セキュリティ監査とシステム監査への考え方（Ｑ＆Ａ）
（いつもより多めに時間を頂いて、自由討議を行ないました。
以下に抜粋、要約して討議の内容を報告します）

Ｑ１）予算はどの程度確保できるのか
Ａ：電子自治体や情報化に関する財政的支援は地方交付税による。

Ｑ２）システム化や監査のアウトソースの状況
Ａ：自治体の場合には、情報化・行政改革といっても、できるだけ地元企業を活用して地域振興を図る目的もある。また監査団体には、専門能力などの資格要件があるが緩やかな条件にせざるを得ない地域もある。現時点では、監査できないよりも実施したほうがいい。

Ｑ３）システム監査
Ａ：全体コストが下がることを示す指標作りから進めたい。

Ｑ４）オープン系のシステムコンソーシアムによる共同開発
Ａ：レガシー連携を目的とした活動のこと。オープン化といっても、必要以上にコストがかかっている場合もあり、何がレガシーかを見直しする必要がある。

Ｑ５）住基カードの普及が進まない
Ａ：先日公表された住基カードの普及率０．２８％は、少ない実績ではあるが、公共団体と住民とのやり取りを電子化するはじめの一歩である。住基カードの多機能化は、準備としては進んでいる。

Ｑ６）市町村合併とＢＰＲ
Ａ：マスコミでは助成金がらみの報道が多いが、特例がないと加速化できないのも事実。自治体ごとの機能統合は、それぞれの現状に合わせて判断される。

Ｑ７）ＩＳＭＳの導入
Ａ：準備は進んでいる自治体も多い。

Ｑ８）総務省ガイドラインと経産省ガイドライン
Ａ：総務省では、まとまったいいものがあれば採用する方針。

Ｑ９）監査報告書の例
Ａ：信頼関係を作るためにも隠したと思われないよう工夫している。

Ｑ１０）事業継続計画
Ａ：作成することになっているが、調査はしていない。新潟地震の場合、バックアップシステムがあっても、長期間の停電では電力がないと何もできないことがわかった。ネットワーク信頼性を上げるにはどうするかの検討を進めている。

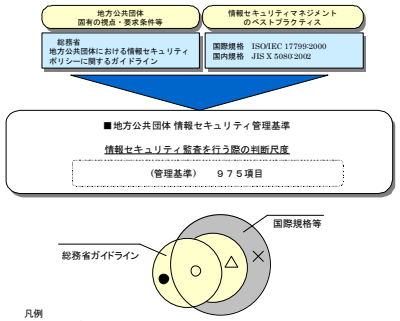
Q11)システム監査を加速するほうが、全体のバランスのとれた電子自治体システム
Ａ：情報セキュリティ対策だけでなく、有効性などの成果を考えると、システム監査は電子自治体システムにとってもバランスのとれた手法であることは理解できるので、研究したい。

以上

（配布資料より）

地方公共団体情報セキュリティ管理基準の概要①

○情報セキュリティ管理基準策定の考え方



凡例

○	総務省ガイドラインに記載され、国際規格等に記載されている項目	６７６項目
●	総務省ガイドラインに記載され、国際規格等に記載のない項目	１８項目
△	総務省ガイドラインに記載がなく、国際規格等に記載されている項目 ただし、監査項目とするかどうかは監査人・地方公共団体の判断にゆだねられる項目	２６６項目
×	総務省ガイドラインに記載がなく、国際規格等に記載されている項目 ただし、地方公共団体の実情からなくても良いと判断される項目	１５項目

地方公共団体情報セキュリティ管理基準の概要②

情報セキュリティ管理基準の構成

項番	マネジメント領域	項目	目的	コントロール（管理目標）	サブコントロール（管理状況）	JIS X 5080	ポリシーの例示	ガイドライン(H15.3)要求事項及び説明	ガイドライン区分	技術的検証項目

地方公共団体情報セキュリティ管理基準は、上記の項目により構成される。

◆ マネジメント領域～サブコントロール(管理状況)

マネジメント領域は、情報セキュリティを確保するために管理すべき領域を定義している（JIS X 5080と同様に10の領域に分類）。それぞれのマネジメント領域はいくつかの目的により構成され、それぞれの目的を達成するために、複数のコントロール(管理目標)とそのコントロールに対応するサブコントロール(管理状況)が設定される。

◆JIS X 5080～技術的検証項目

JIS X 5080～技術的検証項目は、それぞれの管理基準(監査項目)ごとに、以下の点を記載している。

・JIS X 5080(情報セキュリティマネジメントの実践のための規範)との対応関係
・「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15年3月・総務省)との対応関係と地方公共団体固有の要件についての説明
・ガイドラインと対応関係のある項目(ガイドライン区分)
※ ガイドライン区分に該当する項目は総務省が地方公共団体向けに策定・提示しているポリシーとの関連性が高く、他に比して相対的に重要な項目である。
・技術的観点からの検証が可能な項目

地方公共団体情報セキュリティ管理基準の概要③

マネジメント領域～サブコントロール(管理状況)の構造

マネジメント領域	項目	目的	コントロール（管理目標）	サブコントロール（管理状況）
1.セキュリティ基本方針	職務定義及び雇用におけるセキュリティ	人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため	セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること	事件・事故の正式な報告手順を、事件・事故への対処手順とともに確立すること
2.組織のセキュリティ				
3.資産の分類及び管理				
4.人的セキュリティ	利用者の訓練	情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし・・	情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又は・・	事件・事故の正式な報告を受けたならば直ちに取るべき措置に着手できるようにすること
5.物理的及び環境的セキュリティ				すべての職員及び請負業者に、セキュリティ事件・事故の報告手順を認識させておくこと
6.通信及び運用管理			ソフトウェア誤動作を報告する手順を確立すること	
7.アクセス制御	セキュリティ事件・事故及び誤動作への対処	セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため・・・	事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを・	すべての職員及び請負業者に、セキュリティ事件・事故をできるだけ速やかに報告するよう・・
8.システムの開発及び保守				
9.事業継続管理			地方公共団体のセキュリティ基本方針及び手順に違反した従業員に対する、正式な・・	適切なフィードバックの手続を構築していること
10.適合性				

マネジメント領域～サブコントロール(管理状況)の階層構造については、例えば、「4.人的セキュリティ」という領域においては、3つの目的から構成される。それぞれの目的を達成するために、複数のコントロール(管理目標)が設定され、それぞれのコントロール(管理目標)に対して複数のサブコントロール(管理状況)が対応する。

地方公共団体における情報セキュリティ監査の普及促進策

1. 情報セキュリティ監査に関する基準類の管理等のための体制の整備
地方公共団体の主体的かつ継続的な参加による、地方公共団体情報セキュリティ監査ガイドラインの内容に関する適切なメンテナンスを行っていくための体制の整備。

2. 地方公共団体に対する情報提供及び相談のための体制の整備
地方公共団体における情報セキュリティ対策や情報セキュリティ監査の実務等に関して、有用な情報を提供することや地方公共団体からの具体的な相談に応じる等の業務を行うための組織体制の整備。

3. 地方公共団体の共同による情報セキュリティ監査の実施
複数の地方公共団体が情報セキュリティ監査に関する役務を共同で発注することによるメリットや課題等について、今後検討。

4. 情報セキュリティ監査に対する財政支援
情報セキュリティポリシーの策定や情報セキュリティ対策に関連する経費と同様に、地方公共団体による情報セキュリティ監査の実施に要する経費についても所要の地方財政措置を講じる。

5. 地方公共団体における教育・研修等の在り方
職員一人一人が情報セキュリティ対策全般及び情報セキュリティ監査の意義や有効性に対して十分に理解し、進んで実践する高い意識を持つために、職員の能力開発やキャリアパスの形成等に関して、教育・研修等について検討。