平成２２年度ニューメディアを基礎とした調査研究事業
（情報セキュリティガバナンスに関する調査研究）

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と対応策について
調査報告書

平成 23 年 3 月

財団法人ニューメディア開発協会

調査事業者　ビジネスアシュアランス株式会社

KEIRIN

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp

目次

はじめに

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付けになっている。また、昨今では、企業や自治体が相互にネットワークで接続されたり、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や、企業間、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、一部の企業や自治体の情報セキュリティ脆弱性が、ネットワークで接続されている、あるいは共通の情報システムを利用している企業や自治体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る。コンピュータサービスプロバイダをも含めた全体での情報セキュリティレベルの底上げを図ることが益々重要となっており、情報セキュリティガバナンスの確立が欠かせない。

このことを踏まえ、本調査研究では、情報通信技術の発展、普及、環境の変化に対応した情報セキュリティ分野においてガバナンスの確立、維持に必要となる喫緊の課題についての調査研究を行った。具体的には、クラウドコンピューティング等の新サービスをも含めた共通情報セキュリティ基準に関する「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と対応策について」をテーマに調査研究を実施した。

本調査研究の成果として導き出した施策案は、自治体で実際に運用した場合の課題の検証などが更に必要な状況にはあるが、地方自治体が管理する住民個人情報等の重要データのセキュリティ向上の実現に向けて本報告書が利用され、情報セキュリティを実装する際の検討資料として、自治体および IT サービス事業者にとっての一助となることを願うものである。

最後に、本調査研究において検討案作成のための情報提供やインタビュー等に協力をいただいた多くの関係者に対して深く感謝の意を表する次第である。

平成２３年３月

財団法人ニューメディア開発協会
ビジネスアシュアランス株式会社

1. 概要

本事業および本調査研究の背景と目的について、次に示す。

1.1. 本事業の背景と目的

企業や自治体が相互にネットワークで接続されたり、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や、企業間、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。そのためにコンピューティングサービス提供事業者をも含めた全体での情報セキュリティレベルの底上げを図ることが益々重要となっており、情報セキュリティガバナンスの確立が欠かせない。

このことを踏まえ、本事業では、個人情報保護や情報セキュリティへの取組み推進に寄与することを目的として、情報通信技術の発展、普及、環境の変化に対応した情報セキュリティ分野においてガバナンスの確立、維持に必要となる「具体的な情報セキュリティ対策基準の適用課題と対応策について」の調査研究を実施した。

1.2. 本調査研究テーマの課題認識と仮説

自治体が管理する住民個人情報を含む重要情報が、自治体間や地域のサービスとの連携をとりながら利活用される場合に、自治体および自治体より受託して住民個人情報を扱う組織の情報セキュリティレベルが水準以上に保たれていないと、脆弱な部分からの攻撃等の可能性によりその情報交換は漏えいや改ざんなどの脅威にさらされてしまう。また、クラウドコンピューティングや SaaS といった新しい技術を用いたサービスの利用が自治体においてもシステムの運用コスト面や人的資源面の理由から進むものと考えられ、住民個人情報についても、その対象となることは必然と言える状況にある。

昨年度の調査研究（地方自治体における情報セキュリティ対策の具体的な対応基準について）では、全国自治体へのアンケート調査ならびに、自治体で情報セキュリティを推進している担当者の方へのインタビューを通じて、自治体の情報セキュリティ対策レベルの実態を調査し、以下の主たる結果を得た。

①Web アプリケーションのセキュリティ対策等の技術的対策が特に小規模自治体において十分でない

②内外ネットワークの接続パターンの違いによるリスクの大小と実施されているセキュリティ対策レベルとの相関関係が薄い

③外部委託している情報システムの開発やネットワークの十分な文書化や標準化が実施されていない自治体が多い

④約半数の自治体では情報セキュリティ監査や脆弱性の診断といったセキュリティ対策の有効性評価が実施されていない

⑤重要なデータを扱う情報システムの緊急時対応計画の策定を行っていない自治体が、約 40%存在する

⑥教育の実施や重要情報の取扱手順が職員の行動に結びついていない傾向が見える

これらの課題の背景は、担当者の方へのインタビューにおいてその一端が見えたが、「対策をどのレベルまで実施すべきかがわからない、言われてもいない」「予算的に先進自治体のようにはできない」「担当者の育成は定期異動があるのでできない（しない)」「基本的にベンダ任せ」というものであった。

これらの実態調査結果から、

「技術的対策レベルを明確にした」対応基準

「ネットワーク接続形態等のリスクに応じたレベルの」対応基準

「外部委託先に提示できる」対応基準

「監査や脆弱性診断の評価基準となる」対応基準

「職員にもよく理解できる」対応基準

「重要データを扱ううえで全自治体共通で必須となる」対応基準

が必要であり、これらを満足した対応基準が作成され、この基準に各自治体が準拠することで、調査において明らかになった課題が全国自治体一律にクリアできる可能性がある。上述の条件を満足する対応基準を提示し、それにすべての自治体および自治体の外部委託先事業者（クラウドや ASP サービス提供者を含む）が準拠していくことで、住民データ等の重要情報に対する情報セキュリティ対策レベルの向上と一定以上の水準を保つことが可能となり、住民に安全、安心をもたらすことにつながるはずであるという結論に至った。

一昨年度の調査研究（地方自治体における情報セキュリティ対策の実装基準の在り方について）の結果をも含め、昨年度の調査研究で作成した住民個人データ等の重要データを保護するための具体的な情報セキュリティ対応基準の案である「住民データセキュリティ基準（案)」を現実に適用できるものとするための課題は以下のとおりである。

ア）実装基準の位置付けの明確化

地方自治体は、総務省ガイドラインに基づき情報セキュリティポリシーと個別システムの実施手順を作成しているため、対策基準と実装基準の位置付けを明確にする必要がある。

イ）対象となる情報資産の特定

最低限順守すべき情報セキュリティ対策の要件について具体的に規定した実装基準を策定するためには、対象となる情報資産、特にデータ資産を明らかにすることが課題となる。

ウ）条例等との整合性の確保

例えば個人情報に係る重要情報を対象とした実装基準を作成する場合、各自

治体の個人情報保護条例の記載内容との整合性を図る必要がある。このように、条例あるいは他の対策基準等と施策の記述内容が矛盾しないよう、整合性を図ることが課題となる。

エ）技術要件の記載方法

情報セキュリティ対策の要件について具体的に規定することを目的とした場合に、技術要件を記述するための文言が専門用語を駆使したものになり、一般の自治体職員が理解することが難しくなる。このため、技術要件の記載方法が課題となる。

オ）組織体制の検討

例えば個人情報を対象とする場合には、情報システムを所管する部署と個人情報保護を所管する部署の役割分担が重要となる。このため、情報システムを所管する部署と対象情報を所管する部署との役割分担を考慮した組織体制の検討が課題となる。

カ）達成水準の合意形成

例えば、パスワードの構成文字種別および桁数等をどう規定すべきかといった事項について、合意形成を図る手段を検討する必要がある。このため、情報セキュリティ対策の要件について、達成水準の合意形成をどのように図るのかが課題となる。

キ）補助文書等の整備

作成に際しては、実装基準の利用方法等、地方自治体において参照し、活用する際の補助文書等（解説書、評価基準、実施手順等）を整備することが課題となる。

ク）より具体的な内容の記載

情報セキュリティ対策が先行している自治体における具体的な有効事例について、実装基準に反映することが課題となる。

ケ）広範な意見収集と実装基準への反映

より実態を把握した提言（例えば、市町村の実態を把握している都道府県レベルの担当者の意見）等を収集し、実装基準へ反映するための方策が課題となる。

これらの課題をひとつずつクリアしていくことを考えた場合に、クラウドコンピューティングサービスやASPサービスといった新しい技術を用いたサービスの利用が自治体においてもシステムの運用コスト面や人的資源面の理由から進むものと考えられることから、このようなサービスの導入時に、特に住民個人情報等の重要データを扱う場合にサービス提供事業者に対して要求する具体的な情報セキュリティ対策の実装基準の整備が早速に求められている。

このことから、本調査研究では、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の現時点で最重要なものの対応策について検討する必要があると考えた。その結果、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すぐにでも活用することができるものとして、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るという仮説を立てるに至った。この仮説のもとに具体的な検討用の案を作成し自治体担当者やクラウドコンピューティングサービス提供事業者の担当者へのインタビューを通して、その検証を実施することとした。

1.3. 本調査研究成果の想定利用例と期待効果

本調査研究の概要を図 1.1 に、自治体での情報システム（サービス）調達に活用した場合のイメージを図 1.2 に示す。

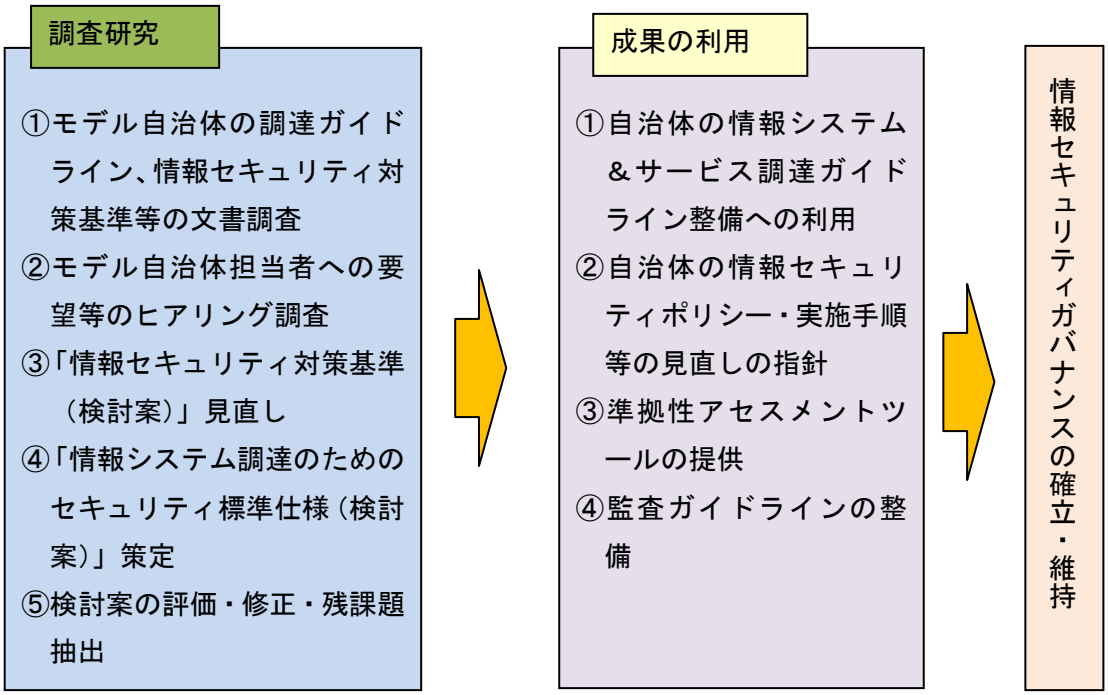

図 1.1　本調査研究の概要

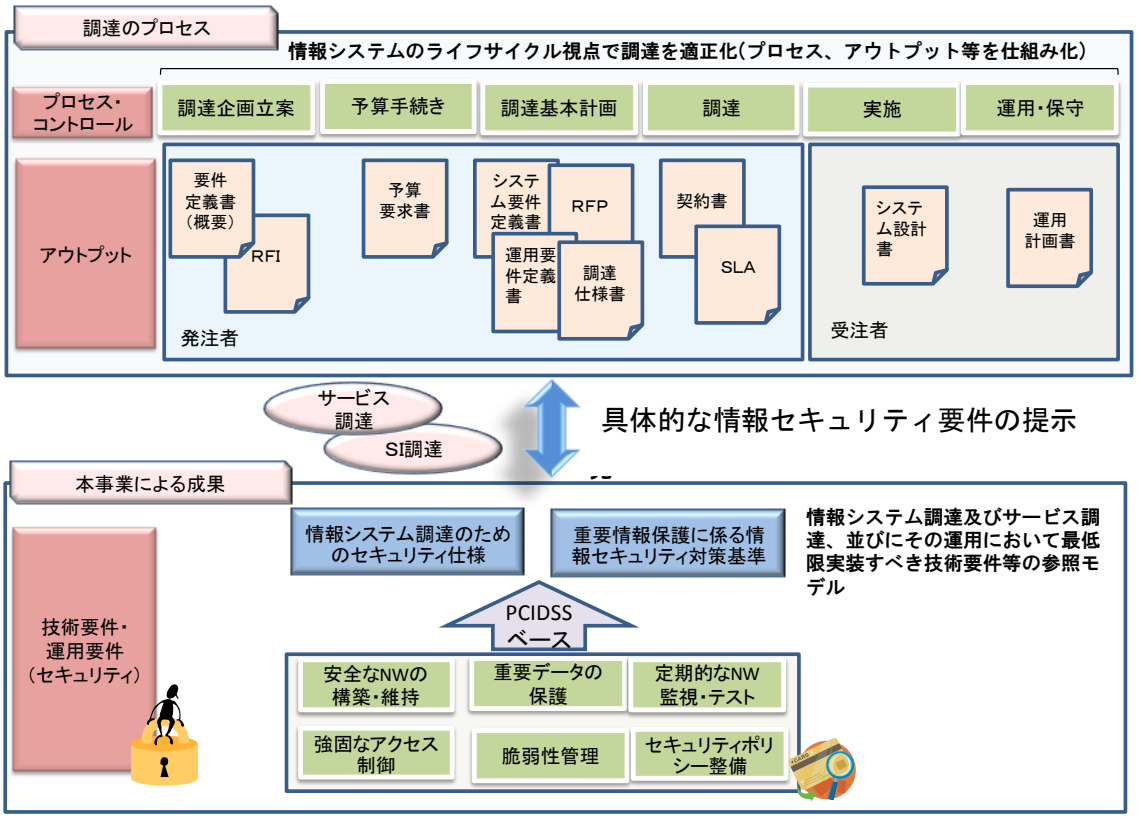

図 1.2　本調査研究成果の活用イメージ

2.　検討方法

2.1.　概要

本調査研究の方法について、次に示す。

本調査研究においては、まずはじめに、モデル自治体を選定し、現状の情報システム調達ガイドラインのセキュリティ要件及び情報セキュリティ対策基準の形式と内容の検証、今後の住民基本台帳法の改正等やクラウドコンピューティングサービス等のアウトソース利用を意識した追加セキュリティ要件の確認及び自治体の要望・意見の聴取を行い、その結果を基にして住民個人情報を取扱う上で最低限遵守すべき具体項目を織り込んだ「情報システム調達のためのセキュリティ標準仕様」及び「情報セキュリティ対策基準」の検討案を作成した。その検討案について、先進自治体とサービス提供事業者の担当者に意見聴取を行い、これらの検討案の完成度を高めるとともに、この一連の検討結果を報告書として取りまとめる作業を行った。

本調査研究は、モデル自治体の文書調査とヒアリング調査、自治体等担当者からの意見聴取、および結果の取りまとめを含む事務局作業により行った。

協力いただいたモデル自治体及び意見聴取先の自治体と事業者のプロフィールを以下に示す。

＜モデル自治体＞

・東京都特別区　A 区

＜意見聴取先＞

・政令指定都市　B 市

・情報システム共同運用実施自治体　C 市

・クラウドサービス事業者　D 社

（世界最大のコンピュータ・ソフトウェア会社）

また、次ページの図 2.1 に本調査研究の手順フローチャートを示す。

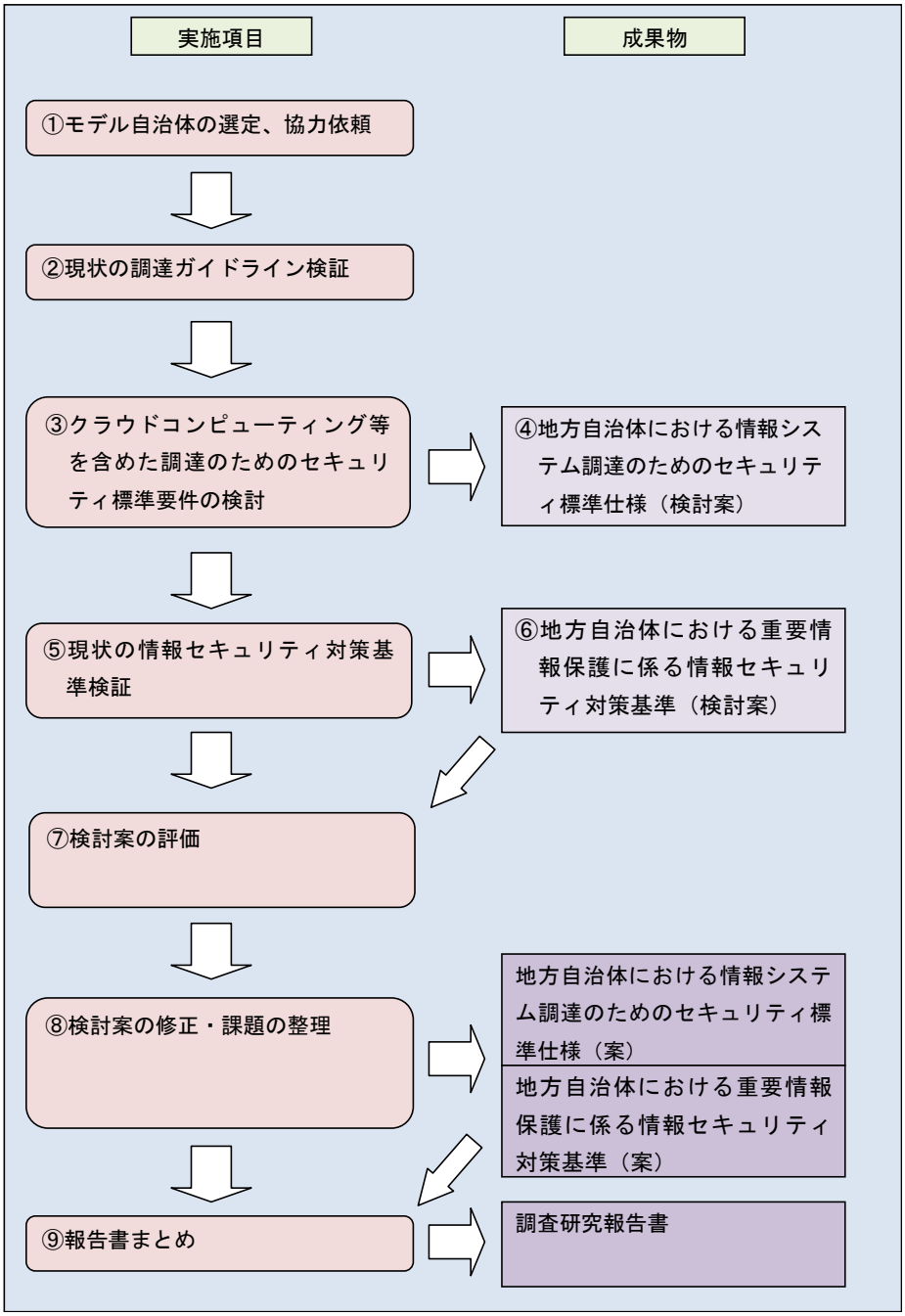

図 2.1　本調査研究の手順フローチャート

2.2. 文書調査

まずはじめに、モデル自治体で使用されている「情報セキュリティポリシー」、「情報セキュリティ対策基準」、「実施手順書」、「情報システム調達時の情報セキュリティ要件提示サンプル」に対し、それらの構成や内容の検証を行った。

2.3. ヒアリング調査

文書調査と並行して、現状の課題認識や状況の変化に対応した要望等を確認するためのヒアリング調査を実施した。

ヒアリング調査は、次の資料を参考にして行った。

・住民データセキュリティ基準案 Ver0.2（検討用）

2.4. 検討案の作成

モデル自治体を対象とした文書調査とヒアリング調査の結果を踏まえた内容の以下の検討案を作成した。

・住民データセキュリティ基準案 Ver0.25（検討用）

・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 Ver0.1（検討用）

2.5. 意見聴取

作成した２つの検討案

・住民データセキュリティ基準案 Ver0.25（検討用）

・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 Ver0.1（検討用）

をもとに、情報セキュリティ対策に関して較的先進している自治体の担当者（課長、課長補佐の方）とクラウドサービス事業者のサービス推進部長に面会の上、意見を聴取した。

2.6. 考察

意見聴取の結果を整理し、その結果に対する考察を実施した。

2.7. 検討案の修正と残課題の整理

考察した結果を踏まえ、検討案の修正と残課題の整理を実施した。

3. 検討結果

3.1. 文書調査及びヒアリング調査

モデル自治体をお願いした A 区の現状の情報セキュリティポリシー、情報セキュリティ対策基準、実施手順（システム所管部門用、利用部門用）及び情報システム調達時の情報セキュリティ要件提示文書に対し、それらの内容を検証した結果と、いくつかの不明点に対して質問し得られた回答内容は以下のとおりであった。

3.1.1. 情報セキュリティポリシー、対策基準、実施手順

①具体的な情報セキュリティ対策基準策定の前提となるリスク分析は実施していない。

②保護すべき情報資産を明確にするための情報資産台帳の作成を行っているが、台帳そのものが十分なものとなっているかの検証はしていない。

③対策基準は総務省ガイドラインベースで作成しており、具体的な対策事項を実施手順に記述しているが、上記①、②の状況であり、リスクに応じた対策強度や守るべき情報資産に応じた基準にはなっていない。

④対策基準の具体化は重要と認識しているが、それ以上に今の基準での対応に対する部門間のバラツキ、管理者や担当職員の認識や対応のバラツキをいかに無くして組織全体での情報セキュリティレベルの底上げを図るかが喫緊の課題と考えている。そのためにセルフチェックや内部監査、外部監査を継続的に実施している。

⑤利用者としての職員に対する基準より、システム所管部門に対する基準の明確化とその遵守が重要となる。情報システム全体の最適化とも関連するが、基幹システムとその周辺システムの情報セキュリティ対策レベルの差の解消が組織全体での情報セキュリティレベル引き上げのための今後の課題と認識している。

⑥対策基準や実施手順の見直しは年 1 回実施しているが、まったくの独自のものとする必然性は感じていない。やはり総務省ガイドラインや ISMS 認証基準を基にしたものとなる。

⑦なぜこの対策をこのレベルまで行わなければならないのかということが一般職員に対して説明できる解説書等は必要である。そのようなものがないと“業務の効率を落としてまで行う必要があるのか“という言い訳に対して説得が難しい。

⑧個人情報を扱う場合、そうでない場合の切り分けは現実的には難しい部分がある。規定は１つで特に個人情報を扱う場合はプラスアルファの対策を必要とするとしたほうがわかりやすい。できるかぎり情報システムを分けて、システム的に個人情報を守るようにすることを考える必要がある。

3.1.2. 情報システム調達時の情報セキュリティ要件

①現状は、調達案件ごとに仕様書に情報セキュリティ要件を記述している。

②契約時には契約書に情報セキュリティに関する遵守事項を列挙した「特記事項」を付けて契約している。ただしこれは汎用的なものであり調達案件毎の内容にはなっていない。
③調達仕様書の原案作成を業者に依頼する場合もある。正直言って情報システムや情報セキュリティのスキル上の問題で自治体職員が作成できるレベルのものでは無い場合がほとんどである。
④情報システム全体の情報セキュリティ対策レベルを合わせる必要があるという観点でも、調達案件毎、提案業者毎、担当者毎に情報システムに求める情報セキュリティ要件が異なるのは大きな課題であることを認識している。この問題を解決するためのアクションを取り始めている。

3.2. 情報システム調達のためのセキュリティ標準仕様案の作成

モデル自治体に対する文書調査とヒアリング調査を経て、上記 3.1.2 情報システム調達時の情報セキュリティ要件の④の“情報システム全体の情報セキュリティ対策レベルを合わせる必要があるという観点でも、調達案件毎、提案業者毎、担当者毎に情報システムに求める情報セキュリティ要件が異なるのは大きな課題”を解決しうる仕様案の作成を行った。

この仕様案は、情報システム等の調達を行う際に「住民データセキュリティ基準案」（以下、「基準案」という）の要求を満たすために、調達の対象となる情報システム等が最低限、実装する必要のあるセキュリティ要件を明らかにするためのものである。

地方自治体の情報システム及びサービス調達の実務において基準案が規定する情報セキュリティに関する要求事項の内容を満たすよう、調達の対象別に必要となる具体的なセキュリティ要件を決定する作業を効率的且つ網羅的に行うことを可能にすることを目的としたものである。

この仕様案が適用される調達の対象となる情報システム等は、次のものを想定している。

① 住民個人データを保有し、住民個人データを保存、処理、伝送するネットワーク及び情報システム並びにこれらを提供するサービス（クラウドを含む）
② 上記①のネットワーク及び情報システム等の運用に係るサービス

この仕様案に掲載しているセキュリティ要件は、基準案の中で情報システム等に対する管理策を定めた「システムの開発、構築、運用者編」の以下のカテゴリー（大項目）を対象として抽出した。

・人的セキュリティ

・物理的セキュリティ
・技術的セキュリティ
・LGWAN、地域 WAN 経由でデータ提供する場合の追加事項
・インターネット経由でデータ提供する場合の追加事項
・暗号化技術と鍵管理
・緊急対応計画

仕様案の中のセキュリティ要件一覧は、下の図 2.2 に示した形式で調達対象毎にセキュリティ要件として必要となる管理策を容易に選択できるようにしてある。

対策基準		調達対象							備考
		ハードウェア等基盤			基盤アプリケーション	個別アプリケーション	運用	設備	
項番	管理策	SW	HW	NW					
	（情報システムの搬出入）								
4.6	管理区域への情報システムの搬出入は、情報セキュリティ責任者の認可なしに実施しないこと。	－	－	－	－	－	－	○	
4.7	管理区域への情報システムの搬出入を行う場合に外部業者が管理区域に立ち入る場合は、同行または立会を行うこと。	－	－	－	－	－	－	○	
4.8	情報システム、データ、ソフトウェアを管理区域から持ち出す場合は、情報セキュリティ責任者の許可を受けること。 4.8.1.持ち出し時および返却時に記録を残すこと。	－	－	－	－	－	－	○	
5.	技術的セキュリティ								
	（アクセス制御）								
5.1.	住民データへのアクセス権限の付与は、業務内容と職責に応じた範囲に制限すること。 5.1.1.特権ユーザ ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されていること。 5.1.2.特権の付与は、個人の職種と職能に基づくこと。 5.1.3.特権ユーザ ID の申請と承認を行う正式な手続きを整備すること。	○	○	－	○	○	○	－	
5.2.	複数のユーザアカウントを持つシステムに対して、ユーザの必要なアクセス範囲に基づいた制限を行うことのできるアクセス制御システムを実装すること。 5.2.1.アクセス制御システムでは、設定時のデフォルトが「すべて拒否」であり、必要に応じたアクセスの許可を行うこと。	○	○	－	○	○	○	－	
	（アカウント ID とパスワードの管理）								
5.3.	住民データを扱うシステムへのアクセスでは、職務の遂行に必要な個人毎に一意の ID を割り当て、ユーザ認証の手法を採用すること。 5.3.1.特権ユーザアカウントは、情報セキュリティ責任者の認可を受けること。 5.3.2.住民データへのアクセスを行うアカウントは、個人毎のユニークな ID を使用すること。 5.3.3.発行されたアカウントは、他人と共有しないこと。 5.3.4.少なくとも 90 日毎に非アクティブなユーザアカウントを削除あるいは無効化すること。 5.3.5.雇用終了、契約終了や異動等によりデータへのアクセス権を失効した場合は、当該ユーザのアクセスを直ちに取り消すこと。	－	－	－	－	－	○	－	

対策基準の管理策

管理策が調達対象に対し調達時のセキュリティ要件に該当する場合は「○」を表記

図 2.2 セキュリティ要件一覧

調達対象の区分は、「「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、地方自治体での調達単位を想定し、また運用管理データセンター等のサービス調達を考慮し、次ページの表 2.2　調達対象区分のとおり分類した。なお、調達対象における小分類に該当するものは、「情報システム調達のための技術参照モデル（TRM）平成 21 年度版」（2010 年 3

月　経済産業書／IPA）を参考に記載した。

表 2.2　調達対象区分

調達対象			備考
大分類	中分類	小分類	
ハードウェア等基盤	ソフトウェア	OS、DBMS、Web サーバ等	
	ハードウェア	サーバ、クライアント PC 等	
	ネットワーク	LAN、WAN、VPN、リモートアクセス、ネットワーク機器等	
基盤アプリケーション	－	認証、統合アカウント管理、ファイルサーバ、グループウェア、電子メール等	
個別アプリケーション	－	個々の業務アプリケーション	
運用	－	サーバ管理、ネットワーク管理等	
設備	－	上記が稼動するための物理的な環境	

3.3.　意見聴取

文書調査及びヒアリング調査で得られたモデル自治体での実使用文書やその使用状況、自治体担当者の課題認識等より、「住民データセキュリティ基準」及び「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」の検討案を作成し、自治体と事業者に意見聴取を行った結果を以下に示す。

① 共同アウトソーシングやクラウドサービスの利用を前提にした場合は、住民個人情報を外部保管する前提となるので、その部分に対してどのような情報セキュリティ要件を提示するかが一番大きな課題となる。
② 自治体クラウド導入のメリット「割り勘効果」を最大化するためにも、クラウドサービス提供事業者に対して求める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が望まれている。
③ 自治体クラウドの現実的な形を意識すると共同アウトソーシング的なものとなるのはある程度理解できるが、その部分をガイドする基準が必要である。たとえば、データセンターの制約や、「共同」の範囲などである。
④ 総務省発行の「ASP・SaaS における情報セキュリティ対策ガイドライン」（ASP・SaaS の情報セキュリティ対策に関する研究会。平成 20 年 1 月 30 日発行）は、参考にする必要がある。

⑤ PCI DSS にはデータセンターに対する情報セキュリティ要求事項の記述が足りないのでこれを補足する必要がある。この部分は「ASP・SaaS における情報セキュリティ対策ガイドライン」を参考にしても良いのではないか。
⑥ クラウドサービス提供事業者側の責任による情報漏えい等のセキュリティ事故に対する補償は、どこの事業者もサービス契約金額内としているはず。
（これで良いのかのガイドラインが必要ではないか）
⑦ 住民データを直接扱わないメールや、一般 OA ソフトのクラウド利用も意識した情報セキュリティガイドラインがあるべきだ。
⑧ 情報システムの調達時のセキュリティ要件は、都度、担当者がチェックしているが、その指標となるものであれば非常に役に立つ。担当者のスキルに依存しないで済むようにすることが必要だと思っている。
⑨ 今の検討案ではイメージがつかみにくい。本当に役立つかはわからない。担当者がチェックする時のチェックリストとして使えるようにしてほしい。そのためには記述がわかりやすい（専門的でない）ことが重要だ。
⑩ いまのところ共同アウトソーシングとかクラウドコンピューティングとかは意識していないが、今後そのような形態のシステムを導入する場合には事前に基準を明確にして準拠していくことが必要だろう。
⑪ 調達対象区分の分類が粗すぎる。もう少し細分化すると現実に使えるイメージになると思う。
⑫ 表に〇が付いているだけでなく、対象となる情報セキュリティ要件だけが抽出され、一覧化されると良い。

3.4. 考察

意見聴取によって得られた意見に対する考察を行った。以下にその内容について述べる。

3.4.1. 「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」の有効性について

（どういう面で有効か）

情報システムの調達時のセキュリティ要件は、都度、担当者がチェックしているが、その指標となるものであれば非常に役に立つ。担当者のスキルに依存しないで済むようにすることが必要だと思っている（B 市）という意見からも、このような形式の情報システム及びサービスの調達時に仕様書に記述する必要のある情報セキュリティ要件は何かが一覧でわかるものが用意できることは有効であることがわかった。なぜなら調達する側の自治体にとって主体的に条件の提示が可能となり、また担当者による判断レベルの差をなくすことが可能になるからである。さらに「住民データセキュリティ基準」を組

織や情報システムに適用することを考えた場合に、情報システム構築時あるいは ASP サービスやクラウドコンピューティングサービスに対しての適用がまず先に必須であるので、これらの情報システムやサービスに対してポリシーや対策基準と合致した要件を調達案件毎に直ちに漏れなく明らかにすることができる点も事業者側の都合や担当者の判断でぶれることが無くなる点で有効と言える。加えて、事業者側から見ても、自治体クラウド導入のメリット「割り勘効果」を最大化するためにも、クラウドサービス提供事業者に対して求める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が望まれている（D 社）という意見のとおり、この標準仕様が共通の基準であれば標準パッケージとして安く提供できる可能性がある。

3.4.2. 「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」の情報セキュリティ要件の記述内容について

（どうすれば使いやすくなるか）

自治体クラウドの現実的な形を意識すると共同アウトソーシング的なものとなるのはある程度理解できるが、その部分をガイドする基準が必要である。たとえば、データセンターの制約や、「共同」の範囲などである（D 社）。PCI DSS にはデータセンターに対する情報セキュリティ要求事項の記述が足りないのでこれを補足する必要がある。この部分は「ASP・SaaS における情報セキュリティ対策ガイドライン」を参考にしても良いのではないか（D 社）。といった意見に対応した「データセンター」に対する情報セキュリティ要件を追加する必要があることがわかった。これについては「ASP・SaaS における情報セキュリティ対策ガイドライン」を参考に検討案に追加することとした。

また、今の検討案ではイメージがつかみにくい。担当者がチェックする時のチェックリストとして使えるようにしてほしい。そのためには記述がわかりやすい（専門的でない）ことが重要だ（B 市）という意見を反映した対応が必要であることが判明した。具体的には調達区分毎の要件リストを容易に作成できる抽出一覧化機能を持ったツールを用意することが必要である。一方、記述のわかりやすさに対しては、わかりやすさに十分配慮した記述にするとともに解説を付ける等の工夫が必要となる。しかしながら情報システムに対する情報セキュリティ要件となると、暗号化手法等そう簡単には書けない部分も残るので運用面での工夫、たとえば CIO 補佐官のアドバイスを得る等の対応が求められる。

さらに、調達対象区分の分類が粗すぎる。もう少し細分化すると現実に使えるイメージになると思う（B 市）という意見への対応も今後の課題として認識した。具体的な自治体での調達単位を調査したうえで現実的な対応が必要である。

3.4.3. 「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」の採用について

（どうなれば現実に適用できるか）

自治体クラウド導入のメリット「割り勘効果」を最大化するためにも、クラウドサービス提供事業者に対して求める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が望まれている（D 社意見）からも、全国統一の基準であることが求められている。全国統一の基準を各自治体が採用するための条件としては、国レベルの強い指導力が必要である。

4. まとめ

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すぐにでも活用することができるものとして、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はないかという仮説は、限られた範囲の意見聴取ではあったが、以下の意見を得たことで概ね正しいことが確認できた。

① 自治体クラウド導入のメリット「割り勘効果」を最大化するためにも、クラウドサービス提供事業者に対して求める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が望まれている。当然、個別対応するよりも標準サービスのほうが安く、かつ均一な情報セキュリティレベルで提供できる。

② 情報システムの調達時のセキュリティ要件は、都度、担当者がチェックしているが、その指標となるものであれば非常に役に立つ。担当者のスキルに依存しないで済むようにすることが必要だと思っている

この結果より、今回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）が今すぐにでも自治体における情報システム調達時の情報セキュリティ要件を考える際に参考として利用できるツールとなりうると言える。

平成 24 年度に予定されている住民基本台帳法の一部改正への対応を機に基幹システムの入れ替えを検討している自治体は多いのではないかと推測している。事実、本調査研究で作成した「情報システム調達のためのセキュリティ標準仕様案」と同様のものを基幹システムの更新タイミングに合わせて自治体独自の基準で作成したいという引き合いが今年度のはじめ（2010 年 4 月）にあった。このようなことを併せて考えれば、この調査研究結果は全国自治体で使える可能性がある。

また一方で、これは住民個人情報を全国一律の基準で保護するという元々の目的を達成するためのひとつのツールにすぎない。達成水準の合意や補助文書等の整備といった残る

課題の解決を図る努力が今後も必要である。

「住民データセキュリティ基準（案）」を中心に、今回作成した「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）」等の関連文書やツールの整備を図って行くことと、要求基準そのものについてのコンセンサスを得ることが今後の大きな課題となる。

引き続き自治体個々での情報セキュリティ強化の努力も当然ながら必要ではあるが、その前提として住民個人情報等の重要データを扱ううえで最低限遵守すべき具体的な基準を全国統一のものとして位置付けることが必要であり、これを実現するための国のリーダーシップが強く求められる。

5. 今後の課題

本調査研究において明らかになった課題とその対応方法等について、以下に記述する。

5.1. 調達対象区分の細分化

今回作成した「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）」では、調達対象区分として「「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、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。

自治体における標準的なアプリケーションをリストし、それぞれについて必要とする情報セキュリティ要件を明らかにできるようにすることが必要となる。

また、クラウドコンピューティングサービスを利用する場合の情報セキュリティ要件をもっと容易に抽出できるようにするための区分の追加が求められている。

5.2. 調達区分毎の要件抽出を容易にするツール化

自治体の情報システム及びサービス調達の実務において、調達の対象別に必要となる具体的なセキュリティ要件の決定を効率的且つ網羅的に行うことを可能にするという目的を達成するには、一覧を見て、〇印が付いている要件をひとつずつ抽出する今の形式では使い勝手が悪い。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るようなツールの作成が必要である。このようなツールがあって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なる。

ツールと言っても簡単なプログラムで作成できる。

5.3. 記述内容のわかりやすさを高めるための工夫

昨年度からの残課題のひとつである。昨年度の調査研究では、「住民データセキュリテ

ィ基準（案)」の管理者編と職員編について分かりやすく記述することに心がけて作成したが、残りのシステム担当者編についても見直し、わかりやすく記述することが求められている。ただし、技術的なセキュリティ要件の記述部分でもあり、この部分の読者はある程度の前提知識があることを想定しているので、誰でもわかるような記述にすることは難しい。したがって要件毎に解説を付ける、あるいはどこまで実施できていればその要件をクリアできるのかを説明した評価基準を追加する等で対応することを検討して課題解決を図ることが必要となる。

要件どおりできない場合の可否判断をどうするか、たとえば CIO 補佐官と相談する等の対応ガイドラインを示すことも考慮に値する。

6. 各種資料

6.1. 参考資料

1) 「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)、平成 18 年 9 月 29 日、総務省
2) 「PCI データセキュリティ基準 要件とセキュリティ評価手順」バージョン 1.2、2008 年 12 月（日本語版リリース)、PCI セキュリティスタンダードカウンシル
3) 平成 20 年度ニューメディア開発協会調査研究報告書
4) 平成 21 年度ニューメディア開発協会調査研究報告書
5) 「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）
6) 「情報システム調達のための技術参照モデル（TRM）平成 21 年度版」(2010 年 3 月　経済産業書／IPA)
7) 「ASP・SaaS における情報セキュリティ対策ガイドライン」(ASP・SaaS の情報セキュリティ対策に関する研究会。平成 20 年 1 月 30 日発行）

6.2. 参考となる URL

1) 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)、総務省
   http://www.soumu.go.jp/s-news/2006/pdf/060929_8_1.pdf
2) PCI DSS の入手サイト
   https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html
3) 「ASP・SaaS における情報セキュリティ対策ガイドライン」
   http://www.soumu.go.jp/menu_news/s-news/2008/pdf/080130_3_bt3.pdf

4) ニューメディア開発協会　平成２１年度ニューメディアを基礎とした調査・研究個人情報保護・情報セキュリティの整備に関する調査研究
http://www.nmda.or.jp/keirin/h21gaiyou/h21kojin-gaiyou.pdf
5) 日本情報処理開発機構
http://www.jipdec.or.jp/
6) 内閣官房情報セキュリティセンター
http://www.nisc.go.jp/active/general/kijun01.html

6.3. 添付資料

【付録 A】情報システム調達のためのセキュリティ標準仕様（案）

【付録 B】住民データセキュリティ基準（案）

以　上

発行日　平成２３年３月
作　成　財団法人ニューメディア開発協会
住　所　〒112-0014　東京都文京区関口１丁目 43 番５号　新目白ビル６Ｆ
電　話　03-5287-5034　ＦＡＸ　03-5287-5029

調査事業者　ビジネスアシュアランス株式会社
住　所　〒140-0002　東京都品川区東品川二丁目２番８号スフィアタワー天王洲

平成２２年度ニューメディアを基礎とした調査研究事業
（情報セキュリティガバナンスに関する調査研究）
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と対応策について

ＵＲＬ：www.nmda.or.jp