Vol.2016-EIP-71 No.7
2016/2/19

基礎自治体の情報セキュリティの現状に関する考察 ~達成度による評価と組織規模との相関~

須藤俊明[†1]　原田要之助[†1]

概要：住民が一番身近に接する基礎自治体の規模は大小様々であるが，その取り扱う情報には機微性があり，政府機関と同様の情報セキュリティ確保が求められる．しかしながら，基礎自治体の情報セキュリティ確保は十分とはいえない．様々な情報セキュリティインシデントの発生やマイナンバー等の新たな制度に向けた安全面への対応は，今後の重要な取り組み課題となっている．

基礎自治体の情報セキュリティ向上策の提案を最終目標として，本稿では初めに，基礎自治体の組織規模の違いや情報セキュリティの現状を明らかにする．次に，先行研究の調査により，自治体の情報セキュリティに関する研究の現状，及び，情報セキュリティレベルの評価基準や手法を把握する．そのうえで，新たに，情報セキュリティの達成度による評価基準を策定し，全基礎自治体に適用して分析を行った．この評価結果を基に，組織規模との相関を調べた．

キーワード：基礎自治体，情報セキュリティ

Study on the present situation of Information Security of the municipality. ‘Correlation of evaluation judgment and organization scale by the achievement degree’

TOSHIAKI SUDO[†1]　YOUNOSUKE HARADA[†1]

Abstract: Regardless of size, every municipality has the obligation to protect residents’ information. Those information contains confidentiality. Therefore, any municipality should ensure to keep the same level of security measures-implemented by the Government. However, security measures taken by municipality may not be enough. Also, various requirements from an increase of security incidents and a new statutes, such as “My Number”, will make security measurements more important subjects.
The purpose of my research is to make a proposal to improve information security of municipality. This paper surveys and discusses about present situation around information security measurements of municipality. Firstly, standards and methodology of security assessment are surveyed by previous researches. Then, correlation between level of security and size of municipality is analyzed by using methodology to assess security level.

Keywords: Municipality, Information　Security

1. はじめに

1.1 研究の背景

住民が一番身近に接する基礎自治体[a]は，安全・安心な行政サービスの提供を要求され，オンライン化や高度なICT 活用が進展している．しかし，基礎自治体においても個人情報漏えい等の情報セキュリティインシデントが頻発している（図 1 参照）．一方で，サイバー犯罪の発生や新たな社会保障・税番号制度（マイナンバー）の導入などにより，基礎自治体の情報セキュリティの重要性がますます高まっている．

2015 年 9 月に閣議決定された「サイバーセキュリティ戦略」[1]においては，自治体は「住民に直結した行政サービスを担う」とし，「十分な対策を講じることが困難な組織」とされている．具体的には「大小様々な規模の団体がありながら，取り扱う情報の機微性などの事情を踏まえれば，政府機関と同様のセキュリティ確保が求められるなどの特別な位置づけにある．」とされており，基礎自治体の情報セキュリティ向上は喫緊な取り組み課題である．

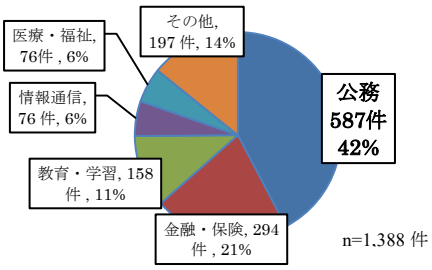


図 1：業種別インシデント件数

引用）JNSA,「2013 年情報セキュリティインシデントに関する調査報告書」より

†1 情報セキュリティ大学院大学
Institute of Information Security.

a）国の行政区画の最小単位で，日本においては市町村及び東京 23 区の特別区を指す．

1.2 研究の目的と概要

研究の最終目標は，基礎自治体の情報セキュリティの向上策を提案することにある．本稿では，図 2 に示すステップで検討を行った．

① 基礎自治体の組織規模（人口規模，財政規模，職員数など）の基礎的条件と情報化推進経費の経年推移・構成内容，及び，情報セキュリティの現状を明らかにする．

② 先行研究を調査し，自治体の情報セキュリティに関する研究の現状，及び，情報セキュリティレベルの評価基準や手法を把握する．

③ 新たに，情報セキュリティの達成度による評価を試み，組織規模との相関を調べる．

それを元に，基礎自治体の情報セキュリティ向上に関する阻害要因の究明や改善の提案を目指す．

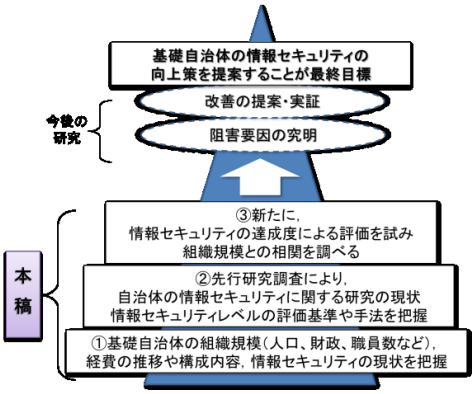


図 2：研究の目的

1.3 達成数，達成率，達成度について

本稿では，総務省の「地方自治情報管理概要」[2]から，情報セキュリティに関連する項目を抽出し，項目を達成している基礎自治体の数を「達成数」，全基礎自治体に占める達成基礎自治体の率を「達成率」としている．また，達成率の大小を，6 段階に区分した度合を「達成度」とする．情報セキュリティの達成度については「4.1 評価項目と判定基準の策定」で述べる．

2. 基礎自治体の規模，情報化推進経費，情報セキュリティの現状

本章では，政府刊行資料により，基礎自治体の人口規模などの基礎的条件や情報化の経費，情報セキュリティの現状を調査し，本研究に必要な基礎数値を明らかにする．

2.1 基礎自治体の人口規模

全国の自治体数は 1,789 団体[b]あり，区分別を表 1 に示す．そのうち，広域行政を行う 47 都道府県を除く 1,742 市区町村の基礎自治体を人口規模別に分類したものを表 2[c]に示す．人口規模については，横浜市の 370 万人を超える大規模自治体から，170 人の青ヶ島村（東京都）まで，大きな差がある．小規模自治体といわれる人口 10 万人未満の基礎自治体は 1,452 団体（以下，小規模自治体），全体の 83.4%にもなる．

表 1：団体区分別団体数

		団体数
都道府県		47
市区町村	特別区	23
	指定都市	20
	市	770
	町村	929
	小計	1,742
合計		1,789

表 2：人口規模別団体数（基礎自治体）

	団体数	構成比	
50万人以上	35	2.0%	
40万～50万人未満	22	1.3%	84
30万～40万人未満	27	1.5%	4.8%
20万～30万人未満	50	2.9%	206
10万～20万人未満	156	9.0%	11.8%
5万～10万人未満	275	15.8%	1,452
5万人未満	1,177	67.6%	83.4%
合計	1,742	100.0%	100.0%

2.2 人口規模別の財政規模，職員数，財政力指数

総務省の「平成 25 年度市町村決算カード」[3]から，人口規模別の財政規模等の数値を表 3 に示す．人口 1 人当たりの経常一般財源[d]は，人口規模が小さくなるほど多くなり，小規模自治体は全体の平均を上回っている．地方税[e]については，人口規模が小さくなるにつれて少なくなり，小規模自治体は全体の平均を下回っていることが分かる．

表 3：人口規模別財政規模等

	団体数	経常一般財源/人口（円）	地方税/人口（円）	一般職員/人口*1000（人）	財政力指数
50万人以上	35	209,434	166,419	6.02	0.77
40万～50万人未満	22	196,181	150,819	5.76	0.80
30万～40万人未満	27	197,248	140,978	5.99	0.75
20万～30万人未満	50	204,454	145,379	6.28	0.77
10万～20万人未満	156	203,413	141,833	6.15	0.75
5万～10万人未満	275	224,742	131,726	6.94	0.65
5万人未満	1,177	304,183	117,968	9.20	0.39
合計/平均	1,742	223,065	144,545	6.68	0.49

また，表 3 に示すとおり，人口 1,000 人当たりの一般職員数[f]についても，小規模自治体ほど多くなり，平均を上回っていることが分かる．

基礎自治体の財政力を示す財政力指数[g]をみると，小規模自治体の財政力指数は 0.7 を割り込み，1,177 団体ある 5 万人未満の自治体では 0.4 を満たしていない．

まとめると，小規模自治体ほど，人的にも，財政的にも効率性が低下し，財政基盤も脆弱であることが分かる．

b) 2014 年 1 月 1 日現在．総務省，「地方自治情報管理概要」より．

c) 2014 年 1 月 1 日現在，住民基本台帳人口．
d) 地方税，地方贈与税，地方交付税など．
e) 市民税，固定資産税，軽自動車税，市町村たばこ税など．
f) 事務・技術職員，除く技能労務，教育，消防，臨時職員．
g)「基準財政収入額」÷「基準財政需要額」で得た数値の，過去 3 年間の平均値．この指数が 1 に近い（あるいは 1 を超える）ほど，財政に余裕があるとされている．「基準財政収入額」は，自治体の標準的な地方税収入額で，税収見込み額の 75%に地方贈与税などを加えたもの．合理的な水準で行政事務を遂行するために必要な「基準財政需要額」とともに，普通交付税の算定に用いられる．

2.3 情報化推進経費の推移と構成内容

総務省の「地方自治情報管理概要」から，基礎自治体の行政情報化推進経費の年度別推移を図 3 に示す．

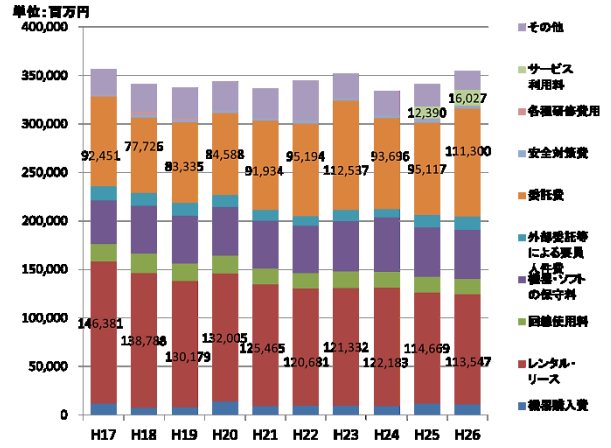
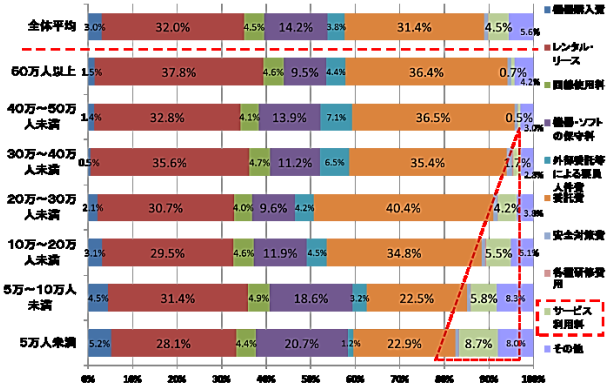


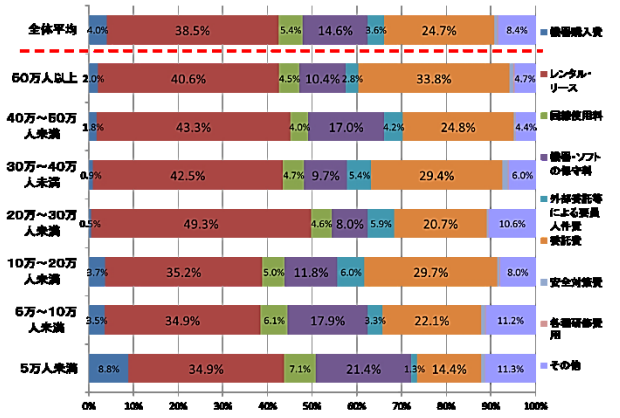
図 3：行政情報化推進経費の年度別推移

レンタル・リースは減額傾向にあり，サービス利用料[h]や委託費は増額傾向にあることが分かる．

次に，平成 26 年度と平成 20 年度の人口規模別の行政情報化推進経費の構成比を図 4 に示す．平成 26 年度の図からは，人口規模が小さくなるにつれてサービス利用率が増加しているのが分かる．



（平成 26 年度予算）



（平成 20 年度予算）

図 4：人口規模別行政情報化推進経費の構成比

h）ASP・SaaS 等のクラウドサービスを利用するための費用．平成 25 年度から調査項目に追加された．

平成 20 年度の図と比較して，傾向と推移をみると，小規模自治体の委託費やレンタル・リース率は，いずれも全体の平均より少なく，機器購入費や機器・ソフト保守料は多いことが分かる．一方，機器購入費や機器・ソフト保守料は減少傾向にあり，委託費やレンタル・リース率は増加傾向にあることが分かる．

図 3・図 4 の傾向から，全体としては外部委託にシフトしていることがうかがえる．また，小規模自治体における，機器購入等による自己運用の割合は，全体平均より多いが，この割合を減らしつつ，クラウドサービス利用に進んでいることがうかがえる．このため、外部委託やクラウドサービス利用対する情報セキュリティ対策の重要度が増している．

2.4 基礎自治体の情報セキュリティの現状

総務省の「地方自治情報管理概要」から，情報セキュリティ対策に関連する項目を抽出し，人口規模別にその達成数及び達成率を集計した．これを表 4～表 6 に示す．なお，表 4・表 5 は情報セキュリティに関連する項目について，PDCA の観点から抽出し，作成した．

表 4：情報セキュリティ計画・実施

	団体数	情報セキュリティポリシーを策定		主要な情報資産について調査及びリスク分析を実施		情報システムの運用等の外部委託先に対する指導・監査を実施		緊急時対応計画を整備		情報セキュリティ研修を職員に対して実施		緊急時対応訓練を実施	
50万人以上	35	35	100.0%	29	82.9%	26	74.3%	32	91.4%	35	100.0%	21	60.0%
40万～50万人未満	22	22	100.0%	14	63.6%	15	68.2%	19	86.4%	22	100.0%	12	54.5%
30万～40万人未満	27	27	100.0%	15	55.6%	22	81.5%	25	92.6%	27	100.0%	14	51.9%
20万～30万人未満	50	50	100.0%	25	50.0%	35	70.0%	38	76.0%	49	98.0%	16	32.0%
10万～20万人未満	156	156	100.0%	76	48.7%	106	67.9%	115	73.7%	150	96.2%	37	23.7%
5万～10万人未満	275	270	98.2%	105	38.2%	150	55.4%	173	63.8%	253	93.4%	62	22.5%
5万人未満	1,177	1,144	97.2%	290	24.6%	483	40.9%	571	48.3%	781	66.1%	152	12.9%
合計	1,742	1,704	**97.8%**	554	**31.8%**	837	**48.0%**	973	55.9%	1,317	76.5%	314	**18.0%**

P（計画）と D（実施）をまとめた表 4 に示すとおり，「情報セキュリティポリシーを策定」している率は 97.8%で，ほとんどの自治体において策定済みとなっている．しかし，「主要な情報資産について調査及びリスク分析を実施」しているのは 31.8%，「情報システムの運用等の外部委託先に対する指導・監査を実施」は 48.0%，「緊急時対応訓練を実施」しているのは 18.0%であった．また，人口規模が小さくなるほど実施率が低いことも分かる．

表 5：情報セキュリティ評価・見直し

	団体数	評価・見直し								情報セキュリティポリシーの見直し状況					
		情報セキュリティについて内部監査のみを実施		情報セキュリティについて外部監査のみを実施		情報セキュリティについて内部監査及び外部監査共に実施		**情報セキュリティについての監査をしていない**		**策定後、一度も見直しを行っていない**		年1回、定期的に実施している		数年に1回、実施している	
50万人以上	35	7	20.0%	3	8.6%	22	62.9%	3	8.6%	1	2.9%	4	11.4%	30	85.7%
40万～50万人未満	22	6	27.3%	3	13.6%	8	36.4%	5	22.7%	3	13.6%	5	22.7%	14	63.6%
30万～40万人未満	27	9	33.3%	4	14.8%	8	29.6%	6	22.2%	3	11.1%	6	22.2%	18	66.7%
20万～30万人未満	50	15	30.0%	2	4.0%	9	18.0%	24	48.0%	11	22.0%	3	6.0%	36	72.0%
10万～20万人未満	156	55	35.3%	11	7.1%	22	14.1%	68	43.6%	32	20.5%	17	10.9%	107	68.6%
5万～10万人未満	275	73	26.5%	23	8.4%	27	9.8%	152	55.3%	82	29.8%	18	6.5%	174	63.3%
5万人未満	1,177	282	24.0%	34	2.9%	69	5.9%	792	67.3%	628	53.4%	40	3.4%	472	40.1%
合計	1,742	447	**25.7%**	80	**4.6%**	165	**9.5%**	1,050	**60.3%**	760	**43.6%**	93	**5.3%**	851	48.9%

情報セキュリティ評価・見直し状況（C・A）を表 5 に示す．「内部監査のみを実施」しているのは 25.7%，「外部監査のみを実施」は 4.6%，「両方実施」しているのは 9.5%で，「情報セキュリティについての監査を実施していない」自治体は，過半数を超える 60.3%となっていることが分かる．

表 5 に示すとおり，情報セキュリティポリシーの見直し状況について，「策定後，一度も見直しを行っていない」率は，情報セキュリティポリシーを策定済み 1,704 団体中の 43.6%で，「毎年 1 回，定期的に実施している」のは，わずか 5.3%にとどまっていることが分かる．次に，表 6 に情報化部門の業務継続計画（ICT-BCP）［4］の状況を示す．「ICT-BCP の策定団体数」は，1,742 団体中の 266 団体，15.3%で，「業務継続訓練をしていない」率は，87.0%となっている．また，特に，小規模自治体ほど策定率が低く，そのほとんどが業務継続訓練をしていないことが分かる．

表 6：ICT-BCP と訓練

	団体数	ICT－BCP策定団体数（初動版のみも含む）		業務継続訓練をしていない	
50万人以上	35	25	71.4%	12	34.3%
40万～50万人未満	22	14	63.6%	3	13.6%
30万～40万人未満	27	17	63.0%	10	37.0%
20万～30万人未満	50	17	34.0%	33	66.0%
10万～20万人未満	156	47	30.1%	107	68.6%
5万～10万人未満	275	47	17.1%	238	86.5%
5万人未満	1,177	99	8.4%	1,113	94.6%
合計	1,742	**266**	**15.3%**	1,516	**87.0%**

まとめると，表 4・表 5 からは，基礎自治体の情報セキュリティ対策を PDCA サイクルでみると，P はほぼ達成状況にあるが，DCA に進むにしたがって達成率が低下し，CA については極めて低く，大幅な改善が必要と考えられる．また，情報セキュリティ対策の達成率については，人口規模により大きな差があり，小規模自治体は他の大中規模の自治体と比較すると，大きく低下する傾向にあることが分かる．そのため，小規模自治体ほどより多くの改善が必要であることが分かる．なお，このことは，組織規模の大きさが情報セキュリティ対策の達成率に影響を与えていることを予測させるが，この検証は 4 章で行う．

3. 先行研究から

先行研究の調査では，初めに，自治体の情報セキュリティの評価について現状を調査する．次に，電子政府・電子自治体の成熟度モデルについて，さらに，情報セキュリティの自己評価について調べる．そのことにより，自治体の情報セキュリティに関する研究の現状や，情報セキュリティレベルの評価基準や手法を把握する．

3.1 自治体の情報セキュリティに関する研究

自治体の情報セキュリティについて，評価手法の研究や情報セキュリティの成熟度モデルの提案，情報セキュリティマネジメントによる分析などが行われている．

林は，「自治体の情報セキュリティ確保のためのザックマンフレームワーク」［5］の中で，ザックマンフレームワーク［i］を利用した情報セキュリティ状態の可視化と改善する手法を提案している．

東川らは「自治体の情報セキュリティに関する成熟度モデル」［6］において，情報セキュリティの成熟度モデルに関して，組織のレベルを判断する指標である COBIT［7］の成熟度モデル［j］等を参考に，表 7 のように提案している．この研究では，2004 年から 2006 年における，自治体の情報化に関する成熟度モデルのデータを，自治体の情報セキュリティにあてはめてモデルの妥当性を検証している．

表 7：自治体の情報セキュリティ成熟度モデル

段　階	内　容	COBIT
5 創出	新しい価値の創出を行う段階	最適化されている(5)
4 評価	情報セキュリティ対策についての効果の評価などを行う段階	管理されている(4)
3 活用	情報技術を活用し、対策を行う段階	定義されている(3)
2 組織	トップマネジメントなど組織の体制の整備を行う段階	再現性あり(2)
1 準備	情報セキュリティ対策を進めるためのインフラの整備を行う段	初期状態(1)
0 不在	情報セキュリティ対策が何もない段階	不在(0)

引用）論文[5]より p2　注）一部省略

しかし，調査項目が十分ではなかったことにより，成熟度の把握が困難であった．そのため，新たな調査項目の提案をしている．

内田の「自治体における情報セキュリティマネジメントの考察」［8］では，ISMS 等の認証制度との関わりから，自治体の情報セキュリティマネジメントの導入状況を分析した．行政に特有の，誤りがないことを前提とした無謬性や，首長の無関心さ等が障害になっていることを指摘している．

3.2 電子政府・電子自治体［k］の成熟度モデルに関する研究

電子政府・電子自治体などの，政府や自治体の情報化を評価する成熟度モデルについては，組織の目標や成果指標の設定，判定手法，進展の阻害要因からの分析，成熟度を決定する組織要因の研究などが行われている．

後藤，須藤は「電子行政の成熟度評価モデルに関する調査研究」［9］において，電子行政（政府）の測定・評価のフレームワークと，成熟度評価モデルに関する研究を行っている．電子行政の目指すべき価値とその業績評価のフレームワークに，行政評価で一般的に用いられている「ロジック・モデル」［l］の考え方を適用した．「民主主義の発展と

i）EA（Enterprise Architecture）を検討するための手法．6 行 6 列からなる表を作成し分析する．
j）IT にかかわる活動を「PO 計画と組織」「AI 調達と導入」「DS サービス提供とサポート」「ME モニタリングと評価」の 4 つのドメイン（領域）に分類している．PO で 10，AI で 7，DS で 13，ME で 4 の計 34 のプロセスを定義し，プロセスごとに実施すべき「コントロール目標」を定め，各プロセスを成熟度レベル（6 段階）で評価する．
k）情報通信技術（IT）を行政のあらゆる分野に活用することにより、国民・住民や企業の事務負担の軽減や利便性の向上，行政事務の簡素化・合理化などを図り，効率的・効果的な政府・自治体を実現しようとするもの．
l）一般に，「資源/インプット」「活動プロセス」「アウトプット」「アウトカム」のドメイン（領域）をもち，「予算」「活動ないしプロセス」「事業ないし施策」「政策ないし戦略」という行政活動と結び付けられる．論理的な因

しての住民参加・透明性の充実度」などの成果指標を用いて,「推進体制」などの 3 つの観点から具体的な有効策を統計的に検証している.

吉田らの「電子自治体における成熟度モデルの構築と適用」[10]では，各自治体が情報化についてどのような成熟度の段階にあるかを分析した．成熟度の上位段階に達するために必要な条件を踏まえ，自治体の新しい成熟度モデルを提案し，市及び区へ適用している.

このモデルの判定基準は，Rogers[11]がイノベーションを採用する場合に用いたカテゴリー分類 [m]を応用している.そして,自治体情報化の目標を「行政内部の効率化」などに設定し，必要なキーファクターを「経営層の関与」などであると結論付けた.

有馬らによる「電子自治体実現に向けての成熟度モデルの構築の試み」[12]では，電子自治体の進展を阻害する要因を分析して，成熟度を定量評価できるモデルの構築について述べている．ここでは，成熟度モデルの試行版の妥当性および適用可能性について，試用した自治体からの評価と感想から，検討している.

あわせて，マイケル・ハマー[13]による「ビジネスプロセスと企業の成熟度モデル (PEMM: Process and Enterprise Maturity Model)」) [n]を参考にした PDCA マネジメントサイクルごとのチェックシート（福岡原則モデル）も提案している.

吉田の「電子自治体の成熟度を決定する組織要因の特定と基礎自治体への適用に関する実証的研究」[14]では，自治体の情報化の成熟度を決定する組織要因を，実証的検証により特定している.「IT 戦略」や「推進体制」などの情報化成熟度を規定する 6 分野の情報化成熟度指標を基にしたモデル分析を行っている.その結果から,「セキュアで効率的かつ利便性の高い情報システムの構築及び運用」を推進するモデルを検証した.そして,組織要因として「IT 化推進能力」と「オープンガバメント志向」の 2 要因を取り出して，それらの相互作用を明らかにしている.

3.3 情報セキュリティの自己評価に関する研究

情報セキュリティの自己評価については，COBIT の成熟度モデルや ISMS 認証基準を基にした研究が行われている.

堀江は「成熟度モデルに基づく情報セキュリティ監査の新たな試み」[15]の中で，監査の「判断基準のゆらぎ」を克服する手法として，COBIT の概念を取り入れた情報セキュリティの成熟度モデルを作成し，監査へ活用することを提唱している．具体的には，NIST の特別報告書 800-26「IT システムのためのセキュリティ自己評価ガイド」[o]を応用した情報セキュリティの自己評価シートを作成し監査に利用することを提案している．表 8 にレベルごとの要求水準を示す.

表 8：要求水準表

レベル	内　　容
第1レベル	コントロール目標が文書化されている段階
第2レベル	セキュリティコントロールが手続きとして文書化されている段階
第3レベル	手続きが導入されている段階
第4レベル	手続きとセキュリティコントロールがテストされレビューされている段階
第5レベル	手続きとセキュリティコントロールが包括的なプログラムとして完全に統合されている段階

引用）論文[14]より p.176

IPA による「情報セキュリティ対策ベンチマーク ver.4.3」[16]はセルフチェックツールである．表 9 に示すとおり 5 段階で評価する.評価項目は 27 項目でトータルスコアの最高は 135 点となる.

表 9：配点表

配点	基　　準
1	経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3	経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4	経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5	4に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

なお，評価項目は，ISMS 認証基準（JIS Q 27001:2006）附属書 A の管理策をベースに作成されている[17].

3.4 先行研究のまとめ

先行研究の調査からは，様々な評価基準や手法があり，多くの成熟度モデルが研究されていることや，成熟度モデルにも様々な手法があることが分かった．また，評価のためには，現状のレベルや，改善するための要件を明確にする必要があることも確認できた．自治体の情報セキュリティレベルを評価するモデルは少なく，一部は提案の段階であることも分かった.

4. 情報セキュリティの達成度による評価試案

本章では，情報セキュリティの達成度による，新たな評価方法を試み，その妥当性について調べる．そのことにより，自治体の情報セキュリティ改善策のヒントを探る.

4.1 評価項目と評価基準の策定

基礎自治体の情報セキュリティのレベルアップを図る

果関係を明示.
m）消費者の商品購入に対する態度をもとに，新しい商品に対する購入の早い順から，5 つのタイプに分類する.
n）5 つのプロセス・ネイブラーと，4 つのケイパビリティを柱として，プロセス・マネジメントにおける組織能力を評価し，ビジネスプロセスの改革を体系的に実行させるツールとなっている.

o）National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce, Computer Security －Security Self-Assessment Guide for Information Technology Systems, （NIST Special Publications 800-26）, Nov.2001.

ためには，自己の現状レベルや，改善するための条件を容易に把握できることが必要である．そのため，3 章に述べた評価基準や手法などを参考に，新たに，情報セキュリティの現状レベルを容易に評価できる基準を策定した．

まず，評価項目については，総務省の「地方自治情報管理概要」から，情報セキュリティ対策を 20 項目抽出した．

表 10：達成度基準表

達成率	達成度
～50%未満	5
50%～69%	4
70%～79%	3
80%～89%	2
90%～	1
未実施	0

次に，各項目の達成数と達成率を抽出し，達成率が低い項目から順に 6 段階に区分し，5 点から 0 点を配点して達成度とした．これを表 10 に示す．

各評価項目に，この達成度基準を適用したものを評価基準とした．これを表 11 に示す．表に示すとおり，20 項目を集計した最高点は 85 点となる．

表 11：評価基準表

項目数		評価項目	達成数	達成率	達成度
		組織体制・規程類の整備			
1		情報セキュリティの責任者や管理者、担当者を任命	1,651	94.8	1
2		情報セキュリティポリシーを策定	1,704	97.8	1
3	P	主要な情報資産について、情報セキュリティ対策実施手順を策定	893	51.3	4
		運用			
4		委託事業者に対し、情報漏えい防止策を契約等により義務付け	1,721	98.8	1
5		情報システムの運用等の外部委託先に対する指導・監査を実施	837	48.0	5
6	D	緊急時対応計画を整備	973	55.9	4
		評価・見直し			
7		情報セキュリティについて内部監査のみを実施	447	25.7	3
		情報セキュリティについて外部監査のみを実施	80	4.6	4
		情報セキュリティについて内部監査及び外部監査共に実施	165	9.5	5
8	C	情報セキュリティポリシー等の遵守状況について、自己点検を実施	786	45.1	5
		情報セキュリティポリシーの見直し状況（※）策定済み1,704を分母			
9		策定後、一度も見直しを行っていない	760	44.6	0
		年1回、定期的に実施している	93	5.5	5
	A	数年に1回、実施している	851	49.9	2
		情報システムに関する業務継続計画（ICT-BCP）の策定状況等況			
10		策定の有無			
		策定している	182	10.4	5
		策定している（ICP－BCP初動版のみ策定）	84	4.8	4
		策定していない	1,476	84.7	0
		策定予定（※）策定していない1,476を分母			
		平成26年度策定予定	147	10.0	2
		平成27年度以降策定予定	587	39.8	1
		策定予定はない	742	50.3	0
11		業務継続訓練の実施状況　（※）策定及び初動版266を分母	266		
		CT部門だけで机上演習を行っている	132	49.6	3
		全庁で机上演習を行っている	13	4.9	4
		ICT部門だけで実地演習を行っている	60	22.6	4
		全庁で実地演習を行っている	12	4.5	5
		関係事業者を含めた大規模な実地演習をおこなっている	9	3.4	5
		災害時の被災者情報管理の業務システムの導入状況			
12		整備済み	568	32.6	5
		整備中	97	5.6	4
		導入予定	212	12.2	2
		導入予定なし	865	49.9	0
		運用管理状況			
13		システム管理者	1,634	93.8	1
14		ファイアーウォール	1,704	97.8	1
15		運用管理規程	1,290	74.1	3
16		障害時マニュアル	947	54.4	4
17		利用者研修	1,268	72.8	3
18		ウイルス対策	1,738	99.8	1
		CISO（最高情報セキュリティ責任者）			
19		任命済み	697	40.0	5
		情報システム台帳の整備			
20		平成25年度までに措置	562	32.3	5
		平成26年度に措置	70	4.0	3
				満点	**85**

この評価基準を 1,742 の全基礎自治体に適用して分析を試みた．また，2 章で調査した人口規模，財政規模，職員数と達成度との相関についても調べた．

4.2 初期分析の結果

4.1 の分析結果を図 5 のグラフに示す．達成度の合計が 70 点以上は 4 団体で，全体の 0.23%，単純平均は 31.53 点，標準偏差は 13.52 となった．これを表 12 に示す．

表 12 の上位の 10 団体をみると，ISMS の認証取得団体が 5 団体[p]（全 6 団体）含まれており，情報セキュリティレベルが高いことが立証された．

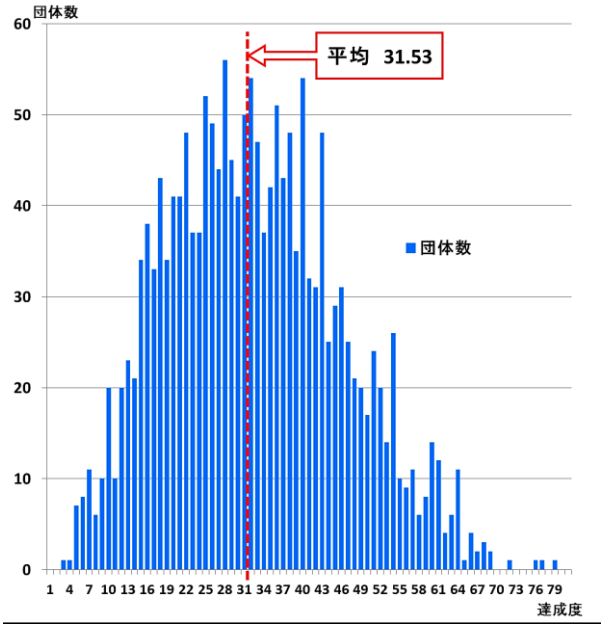


図 5：達成度別団体数

表 12：達成度別団体数

達成度	団体数	率
85～70	4	0.23%
69～55	93	5.34%
54～40	373	21.41%
39～25	696	39.95%
24～0	576	33.07%
計	1,742	100%

単純平均	31.53
標準偏差	13.52

4.3 規模と達成度との相関

4.1 の分析をもとに，人口規模別の達成度のばらつきを図 6 に示す．また，表 13 に示す通り，人口 5 万人未満の小規模自治体の平均値は 27.0 で，全体の平均値 31.5 よりも下回っている．

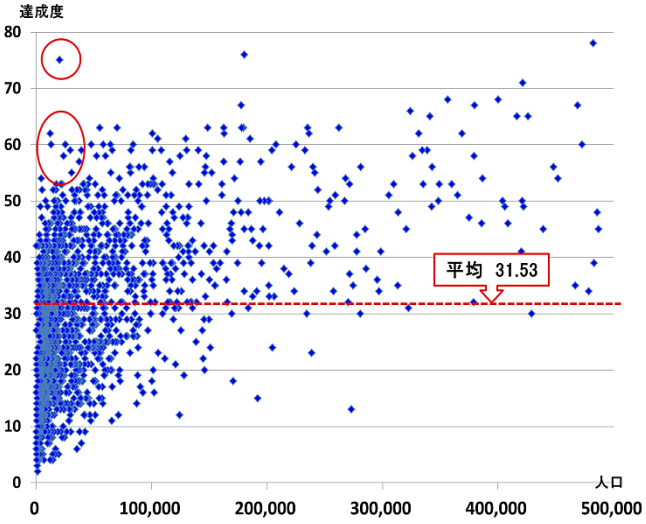


図 6：人口規模別達成度

p）JIPDEC（一般社団法人日本情報経済社会推進協会）より，2015 年 10 月 1 日現在．以下の 5 団体，西宮市，三鷹市，藤沢市，豊中市，市川市．

表 13：人口規模別達成度表

	団体数	達成度平均	達成度				
			85～70	69～55	54～40	39～25	24～0
50万人以上	35	54.5	0	17	17	1	0
40万～50万人未満	22	52.0	2	6	10	4	0
30万～40万人未満	27	53.0	0	11	13	3	0
20万～30万人未満	50	44.0	0	11	20	16	3
10万～20万人未満	156	41.8	1	24	60	58	13
5万～10万人未満	275	36.0	0	15	92	126	42
5万人未満	1,177	**27.0**	**1**	**9**	161	488	518
合計	1,742	**31.5**	4	93	373	696	576

図 6 及び表 13 からは，小規模自治体の改善が全体のレベルアップに大きく貢献することが分かる．

一方，小規模でも，高い達成度を示す自治体が存在する．この理由は現時点では不明であるが．この理由を分析することで，改善のヒントにつなげられると考えている．

最後に，達成度と組織規模との相関については，人口規模，財政規模，職員数及び財政力指数には，ある程度の正の相関が確認できた．一方で，人口当たりの経常一般財源や一般職員数にはある程度の負の相関が確認できた．また，情報システム経費，IT 職員数との相関もあることが分かった．これを表 14 に示す．このことは，2 章で明らかになった基礎自治体の組織規模と情報セキュリティ対策の達成率との関係に合致していた．

表 14：達成度との相関（0.3 以上）

	相関係数
人口規模：2014/1/1現在 住民基本台帳人口	0.39320
経常一般財源：2013年度 市町村決算カード	0.37455
一般職員数：2013年度 市町村決算カード	0.38439
財政力指数：2013年度 市町村決算カード	0.37779
人口当たり経常一般財源：2013年度 市町村決算カード	−0.32683
人口当たり一般職員数：2013年度 市町村決算カード	−0.32527
情報システム経費：地方自治情報管理概要（2014/4/1現在）	0.42920
IT職員数(含む常勤委託要員)：地方自治情報管理概要（2014/4/1現在）	0.38851

4.4「達成度評価」のまとめ

自治体の情報セキュリティのレベルアップを図るためには，自己の現状レベルや，改善するための条件を容易に把握できることが必要である．しかし，自治体の情報セキュリティのレベルを評価するモデルは少なく，一部は提案段階である．

先行研究で参考にされている COBIT の成熟度モデルは，組織の成熟度について，段階を設けて考えることができる重要な指標である．しかしながら，情報セキュリティの評価に関して，成熟度の段階をどのように設定するのか，その妥当性の検証も難しく，利用者の操作性にも一定の熟度が必要と考えられる．また，評価結果を経営陣に説明する場合も，成熟度モデルの説明が必要で，理解を得ることが容易ではないなど，既存の「成熟度モデル」をそのまま自治体の情報セキュリティ評価に適用するのは難しい．

そこで，本稿では，表 11 に示した情報セキュリティについての新たな評価基準（以下，「達成度評価」）を策定して，全基礎自治体を対象に，達成度による分析を試みた．

「達成度評価」は，情報セキュリティについて，総務省が全国の自治体を調査し毎年公開している項目と，その達成率を基にして，評価基準を策定したものである．操作は簡単で，評価項目の実施の有無により達成度を評価する．そのため，恣意的な判断がなく，自己診断も容易に行える．また，全基礎自治体の中の自己のレベルや改善項目を把握できるため，情報セキュリティの知識が十分ではない経営層への説明も容易と考えられる．

また，「達成度評価」による分析結果からは，達成度の上位 10 団体に，5 団体の ISMS 認証取得基礎自治体（全 6 団体）が含まれていることや，組織規模と達成度との相関が確認できたことから，妥当性があると考えている．しかし，達成度の段階ごとの要求特質の定義や，「現在の達成度段階」と「到達すべき達成度段階」との関係などが示せておらず，今後の課題である．

5. まとめ

基礎自治体では，外部委託が増加傾向にあり，クラウドサービス利用も進みつつある．このため，外部委託やクラウドサービス利用に関連する情報セキュリティ確保の重要性が増してくると考えられる．また，小規模自治体ほど，より多くの改善が必要であることが明確になった．

自治体の情報化に関しては，多くの成熟度モデルが研究されているが，情報セキュリティレベルを評価するモデルは少なく，一部は提案段階であった．また，情報セキュリティのレベルアップを図るためには，現時点での自己のレベルや，取り組むべき課題を把握できることが必要であることが分かった．

そのため，新たな「達成度評価」を策定し，全基礎自治体に適用して分析した．その結果，達成度上位に多くの ISMS の認証を取得した基礎自治体が含まれていることや，基礎自治体の組織規模と達成度との相関が検証されたことから，「達成度評価」の妥当性はあると考えられる．

また，「達成度評価」は自己診断も容易に行え，全国の基礎自治体の中の自己のレベルや改善項目も把握できる．さらに，自治体の情報セキュリティに責任を持つ管理者の現状把握や，情報セキュリティの知識が十分でない経営層への説明にも役立つと考えられる．

しかし，達成度の段階ごとの要求特質の定義や，「現在の達成度段階」と「到達すべき達成度段階」との関係が示せていない．この点については，組織のレベルを判断する指標で，組織の現状と組織のあるべき姿を識別することができる，COBIT の成熟度モデルなどを参考に，さらに検討して行く．

また，分析結果から，小規模自治体でも高い達成度を示す基礎自治体が複数存在することも明らかになった．このことから，情報セキュリティの阻害要因については，高い達成度を示す小規模自治体を調査することで，改善のヒントにつなげる考えである．

6. 今後の研究

今後は，本稿により新たに明らかになった課題に取り組むとともに，本稿の結果も踏まえ，基礎自治体の情報セキュリティレベルの向上に影響を及ぼす原因・要因の究明を目指す．そして，最終的には基礎自治体の情報セキュリティの向上に貢献できる提案につなげる予定である．

謝辞

本論文の執筆にあたり，ご指導いただいた情報セキュリティ大学院大学の教授陣，また多くの助言をいただいた原田研究室の客員研究員及びメンバーに対して感謝の意を表します．

参考文献

[1]NISC，「サイバーセキュリティ戦略」，2015 年 9 月 4 日閣議決定.
p.17，「5.2.1 国民・社会を守るための取組，(2)サイバー空間利用者の取組の推進」より.
p.20，「5.2.2 重要インフラを守るための取組，(3)各分野の個別事情への支援」より.
http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf#search='%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%88%A6%E7%95%A5'（2015 年 12 月 31 日閲覧）
[2] 総務省，「地方自治体情報管理概要～電子自治体の推進状況（平成 26 年 4 月 1 日現在）～」． 総務省が毎年全国の自治体を対象に，情報化関連項目を調査し，公表している．
[3]総務省，「平成 25 年度市町村決算カード」，総務省が毎年実施している地方財政状況調査（決算統計）の集計結果に基づいて，各都道府県・市区町村の各種決算状況を 1 枚のカードにまとめたもの.
[4]総務省，「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」及び「ICT 部門の業務継続計画＜初動版サンプル＞」により策定を推奨している.
[5]林隆史，「自治体の情報セキュリティ確保のためのザックマンフレームワーク」，日本社会情報学会誌，2007 年 3 月，pp.73-82.
[6]東川輝久，久保貞也，島田達巳，「自治体の情報セキュリティにおける成熟度モデル」，日本社会情報学会　第 23 回全国大会研究発表論文集，2008 年，PP.338-341 .
[7]ISACA，「COBIT4.1 日本語版」.
[8]内田勝也，「自治体における情報セキュリティマネジメントの考察」，日本情報経営学会誌 Vol.34，No.4，2014 年，pp.130-137.
[9]後藤玲子，須藤修，「電子行政の成熟度評価モデルに関する調査研究」，2008 年.
http://www.taf.or.jp/report/23/index-1/page/p122.pdf
（2015 年 12 月 31 日閲覧）
[10]吉田健一郎，島田達巳，「電子自治体における成熟度モデルの構築と適用」，日本社会情報学会　第 25 回全国大会研究発表論文集，2010 年，pp.297-300.
[11]E・M・Rogers，『Diffusion of Innovations』（邦題『イノベーション普及学』），Free Press ， 1962 年.
[12]有馬昌宏，中土真輝，吉崎智信，山下綾子，島田達巳，「電子自治体実現に向けての成熟度モデルの構築の試み」経営情報学会　全国研究発表大会要旨集，2011 年.
[13]Hammer，M.，“The Process Audit，” Harvard Business Review，April 2007，pp.111-123（邦題「PEMM でビジネスプロセスを改革する」，『DIAMOND ハーバード・ビジネス・レビュー』，2007 年 9 月号，pp.28-45）.
[14]吉田健一郎，「電子自治体の成熟度を決定する組織要因の特定と基礎自治体への適用に関する実証的研究」，電気通信普及財団研究調査報告書 No.28，2013 年，pp.116-123.
[15]堀江正之，「成熟度モデルに基づく情報セキュリティ監査の新たな試み」，会計検査研究，2003 年，pp.171-186.
[16]IPA，「情報セキュリティ対策ベンチマーク ver.4.3」，2015 年 7 月 10 日更新.経済産業省の「企業における情報セキュリティガバナンスのあり方に関する研究会」が 2005 年に取りまとめた報告書により提示されたセルフチェックツール.
「企業における情報セキュリティガバナンスのあり方に関する研究会 報告書 参考資料　情報セキュリティ対策ベンチマーク」，p4.
http://www.meti.go.jp/report/downloadfiles/g50331d01j.pdf
（2015 年 12 月 31 日閲覧）
[17]IPA，「「情報セキュリティ対策ベンチマーク バージョン 4.3」と「診断の基礎データの統計情報」を公開」，2014 年 10 月 27 日.
https://www.ipa.go.jp/security/benchmark/benchmark_20141027.html　（2015 年 12 月 31 日閲覧）