Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

基礎自治体の情報セキュリティ ～達成度評価による向上策の検討～

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，多くの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への対応や，マイナンバー等の新たな制度に対する安全対策は，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的として，本稿では初めに，基礎自治体の規模の違いや情報システム経費の内容，情報セキュリティ対策などの現状を明らかにした．次に，自治体の情報セキュリティに関する先行研究，及び，情報セキュリティレベルの評価基準や手法を把握した．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方法を提案し，全基礎自治体に適用して分析を行った．この評価方法に基づき，組織規模等との相関を確認した．この評価結果からは，インシデントの発生率等との相関が確認され，基礎自治体の情報セキュリティの現状を表していることを確認した．加えて，CISO の任命率は高い相関が確認でき，組織体制の強化が情報セキュリティを高める上で役立つことが分かった．さらに，この評価方法は、使用データの客観性が担保されており，全基礎自治体中の位置づけが把握でき，説明も容易であることから，妥当性があることを確認した．最後に，アンケート調査分析等による今後の研究の進め方について述べる．

キーワード：基礎自治体，情報セキュリティ，達成度，情報セキュリティアンケート調査

Information security of the Japanese municipalities ～ Consideration by the achievement degree evaluation methodology of information security measures to improve ～

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. The security measures for the correspondence to various information security incidents or　the new systems such as“My Number”become a more important action issue.

The final aim of my study is a proposal of the improvement measures for information security of municipality. Firstly, the difference in organization scale, the content of the information system expense and the present conditions of the information security measures of the municipality are clarified in this paper. Secondly, from a precedent study on information security of the municipality, an evaluation standard and the technique of the information security level are grasped. Based on above, the evaluation methodology by the achievement degree of the information security is developed newly, is applied for all municipalities, and analyzed them. Based on this evaluation methodology, the correlation between the achievement degree and the organization size, etc., is confirmed. The evaluation result, which is confirmed the correlation with incidences of information security incident, etc., expresses the present conditions of the information security in the municipality. Especially, the appointment ratio of CISO has a higher correlation with the degree of achievement, it is confirmed that the reinforcement of the organization system has raised the level of information security. This analysis can secure objectivity from use data, and the result can explain easily as grasp one's position in the municipality. The result of methodology can be confirmed that is validity in this analysis. Finally, mention about the future studies such as questionnaire survey analysis.

Keywords: Municipality,　Information Security, Achievement degree, Questionnaire survey

1.　はじめに

1.1　研究の背景と目的

住民が一番身近に接する基礎自治体［a］では，行政の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［b］している．一方で，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，基礎自治体は「住民に直結した行政サービスを担う」ことから，「十分な対策を講じることが困難な組織」とされている．すなわち「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

†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．

b）JNSA,「2015 年情報セキュリティインシデントに関する調査報告書」.

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

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となっている.

1.2 研究の目的と概要

本研究の最終目的は，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．そこで，本稿では，次のステップで検討を行う.

まず，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システム経費の経年推移・構成内容，及び，情報セキュリティ対策の現状を明らかにした.

次に，先行研究により，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した．これらから既存方法の限界が分かった.

そこで，新たに，情報セキュリティの達成度による評価基準を提案し,組織規模や関連する項目との相関を調べた.

研究の最終は，基礎自治体に適した情報セキュリティ向上に資する阻害要因の究明や向上策の提案を目指す.

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，情報セキュリティ対策に関連する項目を抽出し，項目が要求するレベル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．特に，達成率の大小を，6 段階に区分した度合を，新しい検証指標として,「達成度」と定義する．この達成度については「4.1 評価項目と判定基準の策定」に述べる.

2. 基礎自治体の現状

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，情報主管課の情報システム経費，情報セキュリティの現状を調査し，本研究に必要な基礎的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 1,788 団体［c］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 1,741 市区町村の基礎自治体を人口規模別［d］に分類したものを表 2 に示す．人口規模については，横浜市の 372 万人を超える大規模自治体から，167 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 1,453 団体（以下、小規模自治体）であり，全体の 83.5%にもなる.

c）2015 年 4 月 1 日現在，総務省，「地方自治情報管理概要」より.
d）2015 年 1 月 1 日現在，住民基本台帳人口.

表 1 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	928
	小計	1,741
合計		1,788

表 2 人口規模別団体数

	団体数	構成比	
50万人以上	34	2.0%	
40万～50万人未満	23	1.3%	84
30万～40万人未満	27	1.6%	4.8%
20万～30万人未満	50	2.9%	204
10万～20万人未満	154	8.8%	11.7%
5万～10万人未満	270	15.5%	1,453
5万人未満	1,183	67.9%	83.5%
合計	1,741	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 26 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 人当たりの地方税［e］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.

また，表 3 に示すとおり，人口 1,000 人当たりの職員数［f］については，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.

表 3 人口規模別財政規模等

	団体数	地方税/人口（円）	職員数/人口*1000（人）	財政力指数
５０万人以上	34	170,204	8.07	0.78
４０万～５０万人未満	23	156,007	7.47	0.80
３０万～４０万人未満	27	143,819	7.77	0.75
２０万～３０万人未満	50	149,588	8.32	0.78
１０万～２０万人未満	154	144,931	8.10	0.76
５万～１０万人未満	270	135,242	9.36	0.65
５万人未満	1,183	121,092	12.22	0.39
合計/平均	1,741	148,109	8.87	0.49

基礎自治体の財政力を示す財政力指数［g］からは、小規模自治体の財政力指数は 0.7 を割り込み,1,183 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，自治体は小規模ほど，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.

2.3 情報システム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，基礎自治体の情報システム経費（予算ベース）の年度別推移を図 1 に示す.

図 1 からは，基礎自治体のレンタル・リースは減額傾向にあり，ASP・SaaS 等のクラウドサービスを利用するサービス利用料や委託費は増額傾向にあることが分かる.

次に，平成 27 年度と平成 24 年度の人口規模別の情報システム経費の構成比を図 2 に示す.図 2 中の平成 27 年度を見ると，人口規模が小さくなるにつれてサービス利用料の比率（全体に占める割合）が増加していることが分かる.

一方，大規模自治体ではサービス利用料率が低い.

e）総務省，「平成 26 年度決算状況調」より．市民税，固定資産税，軽自動車税，市町村たばこ税など.
f）2015 年 4 月 1 日現在，総務省，「平成 27 年地方公共団体定員管理調査」より.
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.

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

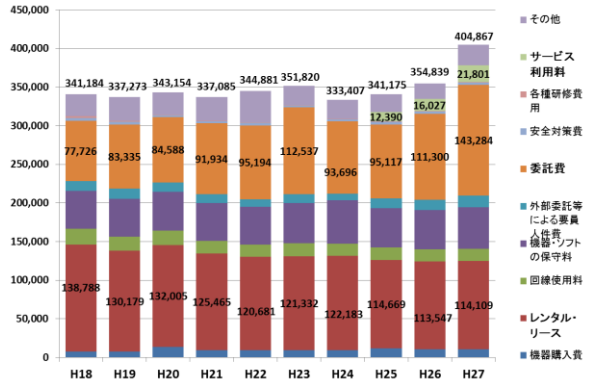

図 1　情報システム経費の年度別推移

図 2 中の平成 27 年度と平成 24 年度の傾向と推移を比較してみると，小規模自治体の委託費やレンタル・リースの比率は，全体の平均より少なく，一方，機器購入費率や機器・ソフト保守料の比率は多いことが分かる．

一方，機器購入費率や機器・ソフト保守料の比率は減少傾向にあり，委託費の比率やレンタル・リースの比率は増加傾向にあることが分かる．

図 1・図 2 の傾向から，全体としては IT システムを独自に構築するのではなく，外部委託にシフトしていることがうかがえる．また，小規模自治体の機器購入等については，

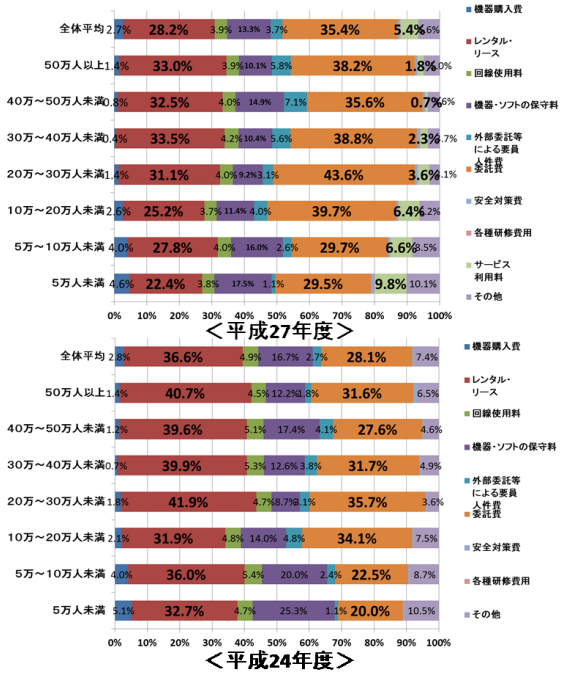

図 2　人口規模別情報システム経費の構成比

自身による構築・運用の比率が減り，クラウドサービスの比率が増えていることから，クラウドの利用に進んでいることがうかがえる．

すなわち，基礎自治体においては，今後，外部委託やクラウドサービスの利用に対する情報セキュリティ対策の重要性が増していると言えよう．

2.4　情報セキュリティ対策の現状

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 と表 5 は情報セキュリティに関連する項目について，PDCA の観点から対応するものを分類して抽出している．

P（計画）と D（実施）をまとめたものを表 4 に示す．表

表 4　情報セキュリティの P（計画）と D（実施）

	団体数	組織体制・規程類の整備						運用					
		情報セキュリティの責任者や管理者、担当者を任命		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、情報セキュリティ対策実施手順を策定		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		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	
		達成数	達成率	達成数	達成率	達成数	達成率	達成数	達成率	達成数	達成率	達成数	達成率
50万人以上	34	34	100.0%	34	100.0%	33	97.1%	34	100.0%	27	79.4%	32	94.1%
40万～50万人未満	23	23	100.0%	23	100.0%	23	100.0%	23	100.0%	16	69.6%	20	87.0%
30万～40万人未満	27	27	100.0%	27	100.0%	21	77.8%	27	100.0%	21	77.8%	24	88.9%
20万～30万人未満	50	49	98.0%	50	100.0%	38	76.0%	50	100.0%	34	68.0%	37	74.0%
10万～20万人未満	154	152	98.7%	154	100.0%	114	74.0%	154	100.0%	106	68.8%	117	76.0%
5万～10万人未満	270	268	99.3%	269	99.6%	169	62.6%	267	98.9%	147	54.4%	178	65.9%
5万人未満	1,183	1,112	94.0%	1,148	97.0%	506	42.8%	1,170	98.9%	493	41.7%	578	48.9%
合　計/平　均	1,741	1,665	95.6%	1,705	97.9%	904	51.9%	1,725	99.1%	844	48.5%	986	56.6%

4 からは，「情報セキュリティの責任者や管理者，担当者を任命」の達成率は 95.6%，「情報セキュリティポリシーを策定」の達成率が 97.9%で，ほとんどの基礎自治体において達成済みとなっている．一方，「情報システムの運用等の

表 5　情報セキュリティの C（評価）と A（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	
		達成数	達成率	達成数	達成率	達成数	達成率	数	率	数	率	達成数	達成率	達成数	達成率
50万人以上	34	6	17.6%	5	14.7%	20	58.8%	3	8.8%	1	2.9%	5	14.7%	28	82.4%
40万～50万人未満	23	5	21.7%	4	17.4%	9	39.1%	5	21.7%	3	13.0%	5	21.7%	15	65.2%
30万～40万人未満	27	8	29.6%	4	14.8%	9	33.3%	6	22.2%	3	11.1%	7	25.9%	17	63.0%
20万～30万人未満	50	17	34.0%	1	2.0%	10	20.0%	22	44.0%	8	16.0%	3	6.0%	39	78.0%
10万～20万人未満	154	51	33.1%	12	7.8%	24	15.6%	67	43.5%	24	15.6%	15	9.7%	115	74.7%
5万～10万人未満	270	77	28.5%	18	6.7%	29	10.7%	146	54.1%	70	25.9%	24	8.9%	175	64.8%
5万人未満	1,183	275	23.2%	33	2.8%	59	5.0%	816	69.0%	574	48.5%	41	3.5%	533	45.1%
合　計	1,741	439	25.2%	77	4.4%	160	9.2%	1,065	61.2%	683	39.2%	100	5.7%	922	53.0%

外部委託先に対する指導・監査を実施」の達成率は 48.5%，「緊急時対応計画を整備」の達成率は 56.6%であった．また，人口規模が小さくなるほど達成率が低いことも分かる．

情報セキュリティの C（評価）と A（見直し）の状況を表 5 に示す．表 5 からは，「内部監査のみを実施」の達成率は 25.2%，「外部監査のみを実施」の達成率は 4.4%、「両方実施」の達成率は 9.2%で，「情報セキュリティについての監査を実施していない」比率は，半数を超える 61.2%となっていることが分かる．

また，表 5 からは，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」比率は 39.2%で，「毎年 1 回，定期的に実施している」達成率は，わずか 5.7%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） 策定と訓練の状況を示す．

表 6 からは，「ICT-BCP を策定している」のは，1,741 団体中の 313 団体，達成率は 18.0%で，「業務継続訓練をしていない」比率は，89.7%となっている．このことから，小規

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

模自治体ほど ICT-BCP 策定の達成率が低く，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 策定と訓練

	団体数	ICT－BCPを策定している		業務継続訓練をしていない	
		達成数	達成率	数	率
50万人以上	34	28	82.4%	18	52.9%
40万～50万人未満	23	14	60.9%	16	69.6%
30万～40万人未満	27	17	63.0%	18	66.7%
20万～30万人未満	50	17	34.0%	41	82.0%
10万～20万人未満	154	53	34.4%	124	80.5%
5万～10万人未満	270	62	23.0%	235	87.0%
5万人未満	1,183	122	10.3%	1,110	93.8%
合　計	1,741	313	18.0%	1,562	89.7%

以上をまとめると，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 とマネジメントの段階が進むにしたがって情報セキュリティ対策の達成率が低下する．一方，CA については達成率が極めて低い．すなわち，CA については大幅な改善が必要と考えられる．また，表 4～表 6 から，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，規模が小さくなると達成率が大きく低下する傾向にあることが分かる．すなわち，小規模な自治体ほど，より多くの改善が必要である．なお，以上の結果から,「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」ことの説明になる．これについては，4 章で詳細に議論する．

3.　先行研究から

自治体（都道府県及び市区町村）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の先行研究について述べる．

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は，いくつかの先行研究があり，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の導入状況の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」[4] の中で，ザックマンフレームワーク [h] を利用した情報セキュリティ対策レベルの可視化と改善するための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」[5] において，COBIT [6] の成熟度モデル [i] 等を参考に，自治体の情報セキュリティ対策レベルの評価手法を提案している．この研究では，2004 年から 2006 年における，基礎自治体の情報化に関する成熟度モデルのデータを，基礎自治体の情報セキュリティの対策レベルにあてはめてモデルの妥当性を検証している．

しかし，一部の段階で調査項目が不足したことにより，成熟度の把握が困難であった．そのため，新たな調査項目を提案し，妥当性を検証している．

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」[7] では，ISMS 等の認証制度との関わりから，基礎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,情報セキュリティマネジメント体制確立の重要性や,行政に特有の無謬性などが障害となっていることを指摘している．

3.2　電子政府・電子自治体の成熟度モデルに関する研究

電子政府・電子自治体 [j] 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」[8] 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」[k] の考え方を適用した．さらに,「民主主義の発展としての住民参加・透明性の充実度」などの成果指標を用いて,「推進体制」などの観点から具体的な効策を提案し，統計的に有効性を検証している．

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」[9] では，各基礎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ている．成熟度の上位段階に達するために必要な条件を踏まえ，基礎自治体の新しい成熟度モデルを提案し，市及び区に適用している．

この吉田のモデルにおける判定基準は，Rogers [10] 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 [l] 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」と設定し，必要となるキーファクターを「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」[11] では，電子自治体の進展を阻害する要因を分析して，成熟度を定量評価するためのモデル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を用いて，基礎自治体に適用し，担当者のヒヤリングにおける感想をもとに，成熟度利用の妥当性および適用可能性について検討している．

あわせて，マイケル・ハマー [12] による「ビジネスプ

h）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．

i）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．

j）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．

k）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．論理的な因果関係を明示．

l）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．

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

ロセスと企業の成熟度モデル（PEMM: Process and Enterprise Maturity Model)」[m] 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」[13]では，基礎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．その結果として，「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」を推進するのに適したモデルを提案している．そして，「IT 化推進能力」と「オープンガバメント志向」の 2 要因の相互作用について述べている．

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」[14]の中で，監査人が異なることでおきる「判断基準のゆらぎ」を克服するために，担当者によらない情報セキュリティの成熟度モデルを考案している．具体的には，NIST の SP 800-26「IT システムのためのセキュリティ自己評価ガイド」[n] 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，監査に応用することを提案している．

IPA による「情報セキュリティ対策ベンチマーク ver.4.3」[15] は自己評価ツールで，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．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[16]に作成されている．しかし，解答にあたっての評価者による判断基準の揺らぎについては対策されていない．

3.4 先行研究のまとめ

以上の先行研究からは，様々な評価基準や手法があり，成熟度モデルについても様々の研究がある．ただし，成熟度モデルを適用して評価するためには，現状のレベルや，担当者が改善するための要件を明確にする必要があること，さらに，評価者によるゆらぎがあることが分かった．一方，基礎自治体の情報セキュリティ対策を想定した評価手法やモデルは少なく，十分に検証されていないことが分かった．成熟度分析についても，実践的な評価まで行われたものはなく，基礎自治体の担当者がすぐに使えるツールとなっていないことが分かった．

4. 情報セキュリティ対策の達成度による評価と分析

そこで，本章では，これらの問題を解決できるものとして，情報セキュリティ対策の達成度を用いた，新たな評価方法を提案し，その妥当性を調べる．

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ためには，自己の現状のレベルや，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が適用できないか検討した．先行研究のどの手法も実際の基礎自治体について，評価者のゆらぎなどにより，統一性のある評価ができないことが分かった．そこで，新たに，情報セキュリティのレベルを容易に評価できる基準を考察した．これを以下に示す．

表 7 達成度基準

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

まず，基本的な基礎自治体の情報セキュリティ項目については，総務省の「地方自治情報管理概要」などが利用できる．しかし，先行研究で多く用いられている成熟度モデルを適用する場合には，各基礎自治体の情報セキュリティに詳しい評価担当者が，直接評価することを前提としている．そのため，他の基礎自治体と共通の指標を用いて，客観的に比較することができない．また，成熟度分析では評価者のスキルによるため，客観的に分析できない．そこで，

表 8 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	1,665	95.6	1
2		情報セキュリティポリシーを策定	1,705	97.9	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	904	51.9	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	1,725	99.1	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	844	48.5	5
6	D	緊急時対応計画を整備	986	56.6	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	439	25.2	3
		情報セキュリティについて外部監査のみを実施	77	4.4	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	160	9.2	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	805	46.2	5
		情報セキュリティポリシーの見直し状況			
9		年1回、定期的に実施している	100	5.7	5
	A	数年に1回、実施している	922	53.0	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	203	11.7	5
		策定している（ICP－BCP初動版のみ策定）	110	6.3	4
		策定予定			
		平成27年度策定予定	117	6.7	2
		平成28年度以降策定予定	605	34.8	1
11		業務継続訓練の実施状況			
		ICT部門だけで机上演習を行っている	150	8.6	3
		全庁で机上演習を行っている	16	0.9	4
		ICT部門だけで実地演習を行っている	76	4.4	4
		全庁で実地演習を行っている	13	0.7	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	13	0.7	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	613	35.2	5
		整備中	109	6.3	4
		導入予定	191	11.0	2
		運用管理状況			
13		システム管理者	1,645	94.5	1
14		ファイアーウォール	1,704	97.9	1
15		運用管理規程	1,304	74.9	3
16		障害時マニュアル	974	55.9	4
17		利用者研修	1,280	73.5	3
18		ウイルス対策	1,737	99.8	1
		CISO（最高情報セキュリティ責任者）			
19		任命済み	998	57.3	4
		情報システム台帳の整備			
20		平成26年度までに措置	586	33.7	5
		平成27年度に措置	60	3.4	3
			達成度合計		**84**

m） 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．

n） 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.

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

客観的な指標である「地方自治情報管理概要」の情報セキュリティ対策項目を用いた評価方法が候補となる．

この評価方法では，まず，「地方自治情報管理概要」から，情報セキュリティ対策を 20 項目抽出する．次に，評価対象となる基礎自治体での各項目の達成数と達成率を抽出する．達成率が低い項目から順に 6 段階に区分し，5 点から 0 点を配点する．これを達成度基準とよび表 7 に示す．この方法では評価者に依存しない点と客観性を担保できる．

表 7 の基準を用いて各項目を評価したものを表 8 に示す．なお，情報セキュリティの監査方法など，1 項目の評価が複数に分かれる場合は，その実施内容に対応する配点としている．

表 8 に示すとおり，20 項目の達成度の合計を「達成度合計」とした．最高点は 84 点となる．

4.2 初期分析の結果

4.1 節の達成度を用いて 1,741 の全基礎自治体の分析結果をグラフに示したものを図 3 に示す．図 3 の横軸は各基礎自治体の達成度合計，縦軸は団体数を示す．また，達成度合計を 5 つの区分に分けて，基礎自治体数との関係を表 9 に示す．表 9 では，達成度合計が 70 点以上は 5 団体で，全体の 0.29%，全基礎自治体の達成度合計の単純平均は 32.53 点、標準偏差は 13.36 となった．

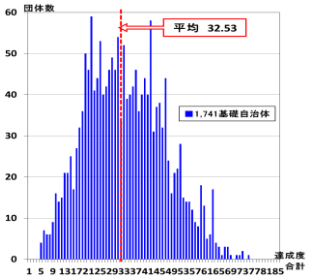

図 3 達成度合計別団体数

表 9 達成度合計別団体数

達成度合計	団体数	率
84～70	5	0.29%
69～55	103	5.92%
54～40	434	24.93%
39～25	650	37.33%
24～0	549	31.53%
計	1,741	100%

全基礎自治体の達成度合計 単純平均	32.53
標準偏差	13.36

表 7 の基準を用いて各項目を評価したものを表 8 に示す．なお，情報セキュリティの監査方法など，1 項目の評価が複数に分かれる場合は，その実施内容に対応する配点としている．

表 8 に示すとおり，20 項目の達成度の合計を「達成度合計」とした．最高点は 84 点となる．

4.3 人口規模と達成度合計

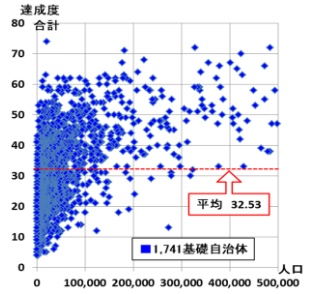

図 4 人口規模別達成度合計

4.2 節の分析をもとに，人口規模別の達成度合計のばらつきを図 4 に示す．横軸は基礎自治体の人口，縦軸はその基礎自治体の達成度合計を示す．また，表 10 に示す通り，人口 5 万人未満の小規模自治体の達成度合計の平均値は 28.1 で，全体の平均値 32.53 よりも下回っている．

表 10 人口規模別達成度合計表

	団体数	達成度合計の平均	達成度合計 85～70	69～55	54～40	39～25	24～0
50万人以上	34	55.9	0	21	13	0	0
40万～50万人未満	23	52.3	2	7	10	4	0
30万～40万人未満	27	52.9	1	11	12	3	0
20万～30万人未満	50	45.1	0	12	22	14	2
10万～20万人未満	154	43.0	1	23	74	46	10
5万～10万人未満	270	37.1	0	17	101	109	43
5万人未満	1,183	28.1	1	12	202	474	494
合計/平均	1,741	32.5	5	103	434	650	549

図 4 及び表 10 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，小規模自治体でも，高い達成度合計を示す基礎自治体が存在する．この理由は現時点では不明であり調査中である．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可能性があり，今後研究する．

4.4 達成度合計の年度別推移

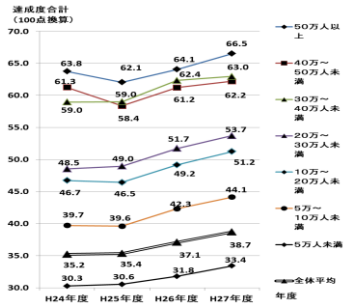

図 5 人口規模別達成度合計の年度別推移

次に，人口規模別の達成度合計の年度別推移を図 5 に示す．

図 5 に示す通り，人口規模に関わらず，毎年，達成度合計が少しずつではあるが改善していることが分かる．

なお，各達成度合計は 100 点換算している．

4.5 インシデントの発生と達成度合計との相関

次に，インシデントが発生し，公表した基礎自治体について，達成度合計の高低と発生との相関について調べた．まず，「Security NEXT」[o] から過去 3 か年度分の基礎自治体のインシデント記事を抽出した．それを基に，達成度合計が平均以上と以下とに区分し，人口 10 万人当たりの発生件数を算出した．これを表 11 に示す．表 11 に示す通り，達成度合計が平均以上の発生件数は 0.24 件，平均以下は 0.99 件となり，約 4 倍の違いがあり，統計的に有意差があると言える．すなわち，達成度合計を高くすることと，インシデントの発生に大きな相関があるので，インシデントを低下させるには，達成度合計を高くすることが有効であると言える．

表 11 インシデント公表基礎自治体の内訳

区分		基礎自治体数	人口	件数	1件当たり人口	人口10万人当たり発生件数
平成27年度	達成度合計 平均以上	37	22,500,288	58	387,936	0.26
	達成度合計 平均以下	12	1,233,370	12	102,781	0.97
平成26年度	達成度合計 平均以上	34	22,743,553	54	421,177	0.24
	達成度合計 平均以下	7	667,484	7	95,355	1.05
平成25年度	達成度合計 平均以上	39	27,372,257	64	427,692	0.23
	達成度合計 平均以下	3	320,227	3	106,742	0.94
3年間計	**達成度合計 平均以上**	**110**	**72,616,098**	**176**	**412,591**	**0.24**
	達成度合計 平均以下	**22**	**2,221,081**	**22**	**100,958**	**0.99**

o) http://www.security-next.com/，2016 年 8 月 11 日最終アクセス．

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

4.6 CISO 任命率と達成度合計との相関

4.3 節の人口規模と達成度合計の分析をもとに，小規模にもかかわらず高い達成度合計を実現している基礎自治体

表 12 大小規模及び高低達成度合計比較

	団体数	人口平均（人）	達成度合計の平均	一般経常/人口（円）	財政力指数	IT職員/人口10万人（人）	人口増加率（%）	情報システム経費/人口千人（円）	住民平均年齢（歳）	IT職員（含む常勤委託要員）（人）	一般職員平均年齢（歳）	一般職員数（人）	CISO任命済（%）	首長年齢（歳）
① 小規模（人口5万人未満）かつ、達成度合計高（55点以上）	9	13,037	60.00	311,650	0.35	23.01	-0.96%	8,506	48.8	3.00	44.3	144	88.9%	71.00
② 大規模（人口30万人以上）かつ、達成度合計低（39点以下）	8	436,615	33.88	192,874	0.85	8.06	0.23%	2,337	44.0	34.13	41.8	2,491	25.0%	57.38
③ 達成度合計高（66点以上）上位11団体	11	356,004	69.91	199,282	0.85	8.56	0.25%	2,970	43.8	26.45	41.8	2,165	90.9%	60.82

と，大規模でも低い達成度合計の基礎自治体，及び，高い達成度合計の基礎自治体を比較した.比較年度については，CISO の任命が初めて調査された平成 26 年度を基準とした.

表 13 CISO 任命率と達成度合計

達成度合計順位（除くCISO評価）	団体数	平均達成度	CISO任命団体数	任命率
1～350	350	48.0	219	62.6%
351～700	350	36.1	156	44.6%
701～1050	350	28.6	134	38.3%
1051～1400	350	21.7	114	32.6%
1401～1742	342	12.8	74	21.6%
合計・平均	1,742	29.5	697	40.0%

比較項目は人口一人当たりの経常一般財源，財政力指数，CISO 任命率，首長年齢などとした.比較項目の中では，CISO 任命率以外に，達成度合計との相関に顕著な違いは確認できなかった．これを表 12 に示す.

また，達成度合計の順位別（除く CISO 評価）の CISO 任命率を調べた.これを表 13 に示す.表 12 及び表 13 からは，CISO の任命が達成度合計と相関があると考えられる．ここでの分析は表面的なものであり，結論にはより細かい分析が必要である.

なお，CISO については，総務省も強力に基礎自治体に設置を要請しており，2014 年 4 月の任命率 40.0%から，2015 年 4 月は 57.3%，2016 年 3 月には 100%［p］となっている.

4.7 達成度合計との相関

表 14 達成度合計との相関

	相関係数
人口規模： 2015年1月1日現在 住民基本台帳人口	0.3966
経常一般財源： 2013年度 市町村決算カード	0.3745
財政力指数： 2014年度 全国市区町村主要財政指標	0.3771
職員数： 2015年4月1日現在 地方公共団体定員管理調査	0.3640
人口当たり職員数： 同上	-0.3150
住民平均年齢： 2010年10月1日 住民基本台帳人口	-0.3496
情報システム経費： 地方自治情報管理概要 2015年4月1日現在、予算額、人口1,000人当たりの情報システム経費	0.4262
IT職員数（含む常勤委託要員）： 同上 2015年4月1日現在、人口10万人当たりのIT職員数	0.3245
職員平均年齢： 地方公務員給与実態調査 2015年4月1日現在	0.0819
人口増加率： 2013年度 市町村決算カード 2014年末と2013年末人口の比較	0.2359

最後に，達成度合計と組織規模との相関について，人口規模，財政規模，財政力指数，職員数との相関関係を調べた．これを表 14 に示す.表 14 より，ある程度の正の相関が確認できた．一方で，人口当たりの職員数や住民平均年齢には負の相関が確認できた．また，表 14 からは，情報システム経費，IT 職員数との相関が見られることが分かった．これによって，2 章で明らかにし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を説明できる.

一方，職員の平均年齢や自治体の人口増加率については，達成度合計との相関は確認できなかった.

4.8 達成度評価の妥当性

本章では，表 8 に示した情報セキュリティについての評価基準を用いて，全基礎自治体を対象に分析を行った.

計算方法は簡単で，評価項目の実施の有無により達成度が評価できる．また，客観的な外部の評価をもとに達成度を計算するため，恣意的な判断がなくなり客観的なものとなる．また，複数年度において比較できるので，自己診断にも用いることができる．さらに，統一的に適用できるので，全基礎自治体の中での，自己の基礎自治体のレベルを把握でき，改善が必要な項目が分かる．このため，必要となる対策が客観的なものとなり，結果として，経営層にとっても分かりやすい.

なお，表 9 の分析結果からは，達成度合計の上位 10 団体に，4 団体の ISMS 認証取得基礎自治体（全 5 団体）が含まれていることや，インシデントの発生との関係が説明でき，組織規模と達成度合計との相関が確認できた．これらのことから，「達成度評価」は基礎自治体の情報セキュリティの現状を表しており，指標として妥当性があると言える．しかし，達成度合計の段階ごとの特質の定義や，「現在の達成度合計段階」と「到達すべき達成度合計段階」との関係が示せておらず，今後の課題が残っている.

5. 今後の研究

今後は，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．ここでは，2010 年から，原田研究室で毎年実施している情報セキュリティのアンケート調査などを活用する.

次に，達成度評価による全基礎自治体の評価結果などから，情報セキュリティの成長モデルを策定し，最終的な目的である，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を検討する予定である.

5.1 達成度合計の官民比較

アンケート調査により，民間企業と基礎自治体とを比較し，情報セキュリティ向上の阻害要因の相違を探る予定である.

2016 年のアンケート調査は，2015 年 8 月に郵送で実施した．対象は，日本国内のプライバシーマーク取得組織，ISMS 認証取得組織，官公庁，教育研究機関などから選んだ，4,800 組織（基礎自治体 398 を含む）である．現時点では 544 の回答がある．なお，設問数は 51 問で，本研究関連は

p）総務省，「地方自治情報管理概要」，平成 28 年 3 月， p.9 より.

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-168 No.13
Vol.2016-SPT-21 No.13
Vol.2016-EIP-74 No.13
2016/11/18

7 問となっている．官民比較の設問については，表 8 に示した基礎自治体の情報セキュリティ評価項目と同様の設問を含んでいる．

また，次の仮説をたてており，分析を進める予定である．

仮説１：ISMS 認証取得企業の達成度合計は極めて高い．

仮説２:中小組織は大規模組織より達成度合計が低下する．

仮説３：CISO の任命は達成度合計に影響する．

仮説４：達成度合計は民間の方が高い．

5.2 情報セキュリティ向上の要因

アンケート調査により，情報セキュリティ対策の実施を阻む要因項目を作成し，その難易度を調べる予定である．考えられる要因には，①コスト要因，②組織要因，③技術要因，④理解要因，⑤効率要因があり，次の 2 つの仮説を検証する予定である．

仮説１：組織規模にかかわらず，情報セキュリティ対策の阻害要因傾向は変わらない．

仮説２：中小組織は大規模組織と比較して，コストや技術に困難性を感じている．

また，4.3 節で述べた人口規模と達成度合計の分析から明らかになった，高達成度合計の小規模自治体について，個別にアンケート等によりその要因を調査する予定である．

本研究では、組織における情報セキュリティ対策の実施主体である，情報セキュリティ責任者・担当者を対象にしている．情報セキュリティへの阻害要因や推進要因が明らかになることで，基礎自治体やその担当者がどのように行動すれば良いかについて自分で判断できることを目指す．

また，組織規模による比較により，特に，小規模自治体が困難と感じている要因を明らかにして，情報セキュリティレベルの向上に寄与することを目指す．

5.3 情報セキュリティ向上策の提案

4.8 節の達成度評価の妥当性で課題となっている，達成度合計の段階ごとの特質の定義や，成長モデルの策定，成長段階別のナビゲーションの提案を目指す．

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，p.20.

[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 27 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 26 年度市町村決算カード」．総務省が実施している地方財政状況調査（決算統計）の集計結果に基づき，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] 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.

[5] 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.

[6] ISACA,「COBIT4.1 日本語版」.

[7] 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.

[8] 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 日アクセス

[9] 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.

[10] E・M・Rogers,『Diffusion of Innovations』(邦題『イノベーション普及学』)，Free Press，1962 年.

[11] 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.

[12]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）.

[13] 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.

[14] 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.

[15] 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.

[16]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.

[17] 原田要之助,「大規模な情報漏えい事件の特性と対策の考え方」情報セキュリティ総合科学，第 4 号 2012 年 11 月.

[18] 村上靖，内田勝也,「情報セキュリティ事件・事故の分析と対策に関する考察」,情報処理学会研究会報告, 2010 年 3 月.

ⓒ2016 Information Processing Society of Japan