基礎自治体の情報セキュリティ
ー達成度評価と向上策ー
Information security of the Japanese municipalities
- An achievement degree evaluation methodology and improvement measures -

須藤　俊明・ネットワーク分科会・情報セキュリティ大学院大学

Abstract: ″An achievement degree evaluation methodology″ that the current information security level can be evaluated based on ″Local Autonomy Information Management Overview″ announced annually by the Ministry of Internal Affairs and Communications is proposed.
The evaluation method has been applied to all the basic municipalities and analyzed, and the validity of this method is confirmed.
In addition, ″An achievement degree growth model″ and ″An achievement degree growth navigation″ are proposed. As a result of them, the person in charge can image each level concretely, and grasp the measures that need to be taken next easily.

1．研究の概要

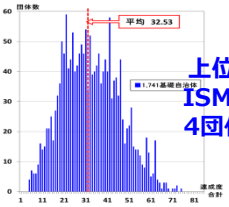
①本研究では、基礎自治体（全国の1,741市区町村）の組織規模と情報セキュリティの現状を調査し、情報セキュリティ向上は、喫緊の取り組み課題であることを明らかにした。
②次に、先行研究から、情報セキュリティの向上には、現状レベルが評価でき、成長のレベルが示せ、次のレベルに進む道筋を明らかにする必要があるが、担当者が容易に利用できるツールはないことが分かった。
③そこで、総務省が毎年公表する**「地方自治情報管理概要」**をベースに、現状の情報セキュリティのレベルを評価できる**「達成度評価」**を提案し、全基礎自治体に適用・分析して、その妥当性を確認した。
④また、「達成度評価」や「難易度」を用いた官民比較により、情報セキュリティ向上の要因を探った。
⑤次に、**「達成度成長モデル」**や**「達成度成長ナビ」**を提案した。これにより、担当者は各レベルを具体的にイメージでき、次に取り組むべき対策も容易に把握できる。
⑥これら3つのツールは、担当者のスキルが不要で、簡単に操作でき、揺らぎがなく、すぐに使えるツールとなっている。
また、基準の陳腐化を防ぐことができ、更新の際の煩雑性や恣意性も排除され、客観性も担保される。

2．「達成度評価」と妥当性

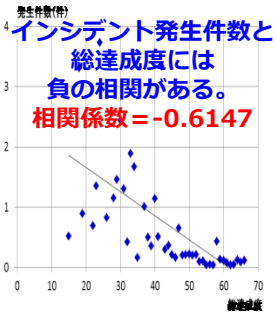
「地方自治情報管理概要」から、情報セキュリティ対策の評価項目（２０項目）を抽出。　評価項目の**「達成率」**から、達成率が低い順に５点～０点を配点**「達成度基準」**とする。

達成度基準を評価項目に適用し**「評価基準」**とした。

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



上位の10団体には、ISMS認証取得団体が4団体含まれている。



インシデント発生件数と総達成度には負の相関がある。
相関係数＝-0.6147

項　　目	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	0.3725
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 人口1万人当たりの職員数	−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

組織規模との相関が確認できる。

3．「達成度評価」「難易度」による官民比較

組織別の平均達成度計

アンケート調査組織	組織数	平均達成度計	備　考
CISO任命　かつ ISMS認証取得組織	99	47.28	民間企業95組織、基礎自治体2組織、他の公務2組織（基礎自治体中50.0）
CISO任命 企業	130	44.30	除く公務、大学
ISMS認証取得 企業	172	42.80	
CISO任命 組織	225	40.50	
中堅・大企業	29	40.52	
CISO任命 基礎自治体	57	36.51	
民間企業	362	35.00	
中小企業	333	34.51	
基礎自治体	76	34.37	
全調査組織	544	32.78	
Pマーク取得 企業（除くISMS）	186	27.54	
大学	66	17.31	
<参考：表23より> H27年度基礎自治体の達成度計	1,741	24.85	平成27年度の基礎自治体を、表21の13評価項目の評価基準で評価した平均達成度計

※平均達成度計：調査組織の各評価項目の平均達成度の合計。

基礎自治体は、ISMS認証取得やCISO任命、「評価」や「見直し」に努めることが、情報セキュリティ向上につながると認識する必要がある。

組織別の難易度平均

アンケート調査組織	組織数	難易度平均	備考
ISMS認証取得 企業	172	2.85	
CISO任命 企業	130	2.85	
中小企業	333	2.86	
CISO任命かつ ISMS認証取得組織	99	2.87	
民間企業	362	2.87	
Pマーク取得 企業（除くISMS）	186	2.89	
全組織	544	3.04	
中堅・大企業	29	3.04	
大学	66	3.43	
CISO任命 基礎自治体	57	3.49	
基礎自治体	76	3.52	

平均達成度計と難易度平均との相関は確認できなかった。
情報セキュリティ対策の実施は、情報セキュリティのレベルにかかわらず困難性を伴っていると考えられる。

4．「達成度成長モデル」「達成度成長ナビ」

達成度成長モデル

成長段階	定　義	要　件（達成項目）	後達成度の目安	特記事項
5	情報セキュリティに対する執認・見直しが習慣に行われている段階	ISMSの認証取得、PDCAサイクルの実施 内部監査及び外部監査の実施、リスク分析の実施 IOT・SOP（業務標準計画）の策定、ポリシーの定期的見直し 組織時や業務環境の調査の実施 情報システム資産の整理、監査データの電子化の実施	65以上	・ISMSの認証を取得すること ・PDCAサイクルを環境に実施すること ・常時に見直しを実施すること
4	情報セキュリティに対する自己点検や改善のルール化の段階	自己点検の実施 外部監査人の指導の実施、内部監査の実施 実施手順書の策定、標準書マニュアルの策定 SPF（治安ドメイン監査）の実施	55以上	・監査や自己点検など、評価を常時に実施すること
3	情報セキュリティに対する組織間連携や業務間の対策を行う段階	組織間対応計画の策定 CISOの任命 クラウドサービスやデータセンターの活用 監視管理部署の設置と利用者研修の実施	40以上	・CISOを任命し、組織部署が協会すること ・情報セキュリティ担当者等、庁内の管理者を組織化し機能整理すること ・緊急時を想定した計画を整備し、訓練を実施すること
2	情報セキュリティに対する組織体制整備の段階	情報セキュリティ研修の実施 アクセスログの長期・状態、組織体の設計管理の実施 USBメモリなどの持ち出し制限の実施 未許可ソフトウェアの導入禁止 システム管理者の任命 情報セキュリティ責任者や管理者、監査者の任命	25以上	・情報セキュリティの重点指導、責任者等を任命すること ・LGWAN（地方公共団体情報システム協議）が実施する eラーニングを利用すること ・「ヒヤリハット」などと助対策を実施すること
1	情報セキュリティに対する基礎整備の段階	情報資産の無断持ち出しやメール送付の禁止 アクセス制限の実施、機器廃棄時のデータ処理の実施 サーバ設備の入出制限、停電対策の実施 情報セキュリティポリシーの策定 ファイアーウォール、ウイルス対策の実施 重要データのバックアップ取得の実施 機器等管理簿に設備置入い出と使用者等で機器付けの実施 不正プログラム対策ソフトや定期ファイルのアップデートの実施	—	・サーバー室の入退出を制限すること ・パソコンの利用制限を実施すること
0	情報セキュリティに対する対策がない段階	対策なし	—	

自己評価するための「達成度評価シート」に評価項目の達成の有無を入力するだけで「達成度成長ナビ」が自動作成される。

達成度評価シート

評価基準項目	評価項目 ＼ 成長段階	達成率	達成度	自己評価 達成の有無	自己評価 達成度	備考
1	情報セキュリティの責任者や管理者、監査者を任命	98.6	1			
2	情報セキュリティポリシーを策定	97.0	1			

情報セキュリティの自己評価による総達成度をもとに、成長段階を把握する、目安とすることができる。

達成度成長ナビ

評価基準項目	評価項目 ＼ 成長段階	5	4	3	2	1	達成率	達成度	自己評価 達成の有無	自己評価 達成度
11	業務組織間連携　全庁で実地調査	40.0%	2.9%	1.4%	0.3%	0.0%	0.7	5		
11	業務組織間連携　関係者を含めた大規模な実地調査	40.0%	8.7%	0.8%	0.0%	0.0%	0.7	5		