

情報セキュリティ対策ベンチマークの4年間の診断の基礎データより

情報セキュリティ対策状況の経年比較

2010年6月29日

2008年4月より、情報セキュリティ対策ベンチマークの診断の基礎データについては、情報セキュリティを巡る環境変化やレベルの変化を勘案し、最新2年分のデータを適用することとし、毎年、基礎データの入れ替えを行うようになりました。

本紙では、表2に記載の4年間の診断データに基づき、企業規模別の情報セキュリティ対策状況を経年比較したデータを示します。なお、ここでは、従業員数300名を超える企業を大企業といい、300名以下の企業を中小企業といいます。

1. 情報セキュリティ対策ベンチマークの診断の基礎データと4年間の診断データ

情報セキュリティ対策ベンチマークの診断の基礎データの件数を表1に、2006年から2009年までの各年度の診断の基礎データの件数を表2に、各年度の診断の基礎データの従業員数の分布を図1に示します。

表1 情報セキュリティ対策ベンチマークの各バージョンで適用する診断の基礎データ^{※1}

バージョン	リリース日	適用する診断の基礎データの期間	基礎データの件数
Ver.3.1	2008/4/21	2006/3/20～2007/12/17(約2年間)	2165
Ver.3.2	2009/5/22	2007/1/1～2008/12/31(2年間)	1974
Ver.3.3	2010/6/29	2008/1/1～2009/12/31(2年間)	1540

※1:このデータでは、毎年診断しても、1件として扱われます(最新の診断データを使用)

表2 診断の基礎データを1年毎および企業規模別に分けた場合の件数^{※2}

年	使用データの期間	全データ件数	データ件数 (中小企業)	データ件数 (大企業)
2006年	2006/3/20～2006/12/31	1053	662	391
2007年	2007/1/1～2007/12/31	1165	674	491
2008年	2008/1/1～2008/12/31	930	550	380
2009年	2009/1/1～2009/12/31	808	466	342
	合計	3956	2352	1604

※2:このデータでは、毎年診断する企業は、各年度の数に含まれます。

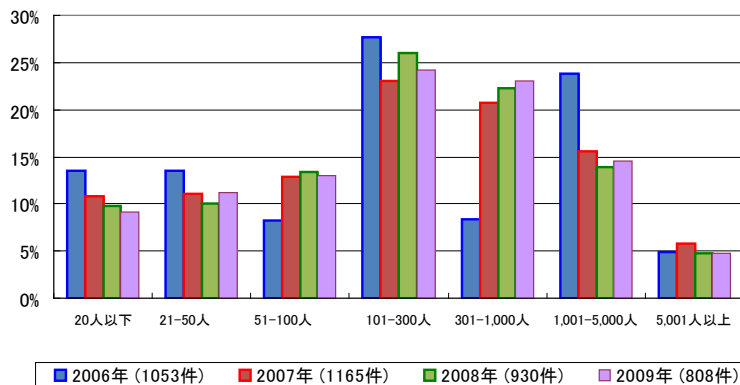


図1 4年間の診断の基礎データの従業員数の分布

2. 全体の情報セキュリティ対策状況の経年比較

全体の各年度のトータルスコア¹平均等一覧を表3に、情報セキュリティ対策25項目のスコア平均の経年比較を図2に、情報セキュリティ対策25項目スコアの分散の経年比較を図3に示します。分散や標準偏差は、その項目におけるスコアのばらつき度合を示し、値が小さいほどばらつきは少なくなります。

トータルスコアの平均や評価項目25項目のスコア平均は、毎年向上し、情報セキュリティリスク指標²の平均は、毎年高くなっています。2009年度は、トータルスコアや各項目平均の向上の度合いが他の年度よりかなり高くなっています。また、トータルスコアの標準偏差や情報セキュリティ対策25項目スコアの分散を見ると、2007年は他の年度と比較してばらつき具合が大きくなっています。情報セキュリティ対策25項目で、2006年と2009年を比べて、向上の度合いが大きい(項目スコア平均の差が大きい)のは、上から順に、「第三者アクセス」、「建物等のセキュリティ」、「媒体の紛失・盗難対策」、「開発時のセキュリティ」、「従業者との契約」であり、あまり変化がないのは、変化の少ない順に、「不正プログラム対策」、「情報の工程毎の安全対策」、「脆弱性対策」、「障害対策」です。不正プログラム対策は、取り組みがすでに進んでいることにより差がない項目であり、情報の工程毎の安全対策は、取り組みにくい項目であるため、対策が進まない項目と考えられます。事業継続への取り組みは、各年度を通じて、25項目の中では取り組みが一番遅れている項目です。

表3 各年度全件のトータルスコア平均等

	トータルスコア		評価項目 スコア平均	リスク指標平均	件数
	平均	標準偏差 ^{※3}			
2006年	73.349	19.63	2.934	-0.073	1053
2007年	75.658	21.07	3.026	0.559	1165
2008年	78.082	19.74	3.123	0.784	930
2009年	83.630	20.37	3.345	1.097	808

※3:標準偏差は統計値の散らばり具合を表す数値です。標準偏差は、分散の正の平方根です。

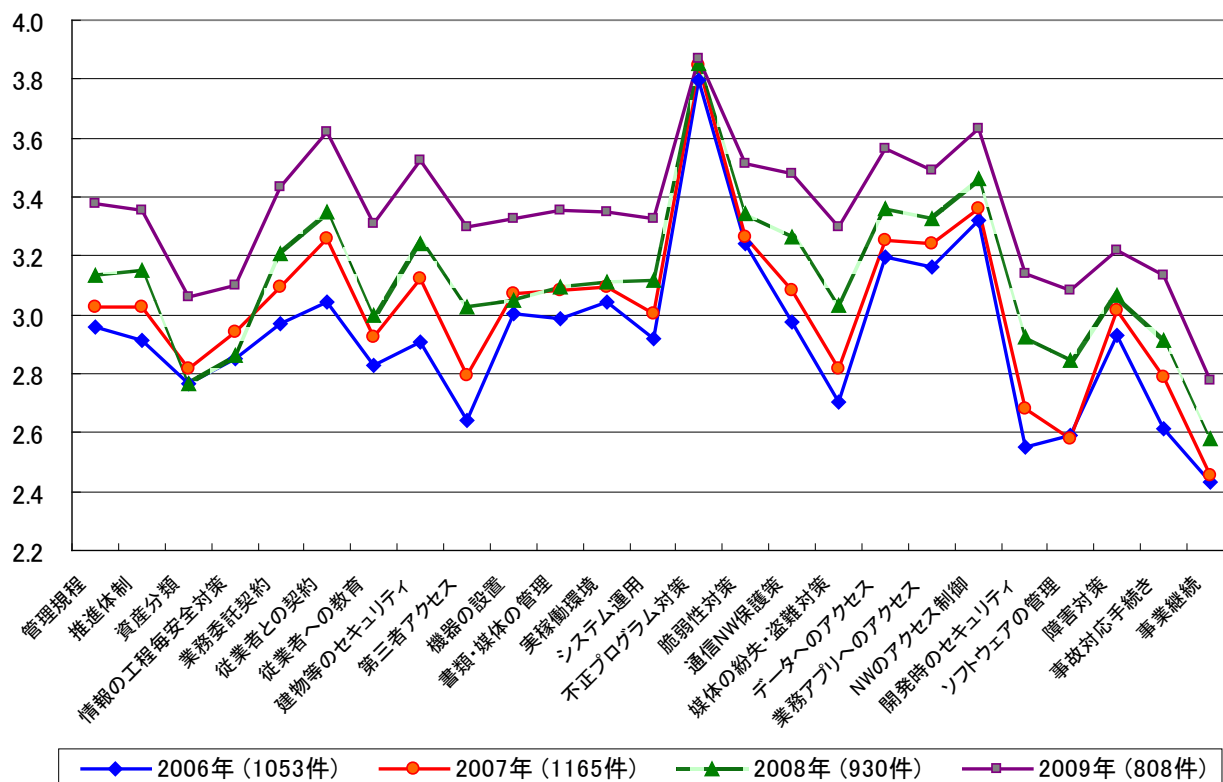


図2 情報セキュリティ対策25項目のスコア平均経年比較^{※4}

(※4:各項目のスコアは1点から5点ですが、この図では比較のため、2.2点から4点までを表示しています。)

¹情報セキュリティ対策の実施状況に関する25問へ5段階で回答すると、スコア(点数)が計算されます。各評価項目は5点、トータルスコア(合計点)は125点です。75点を各項目に均すと3点になります。3は「実施しているが、実施状況の確認はしていない」という状況を表します。

²情報セキュリティリスク指標は、従業員数、重要情報の保有数、IT依存度などから計算される企業のかかえるリスクを表す指標です。

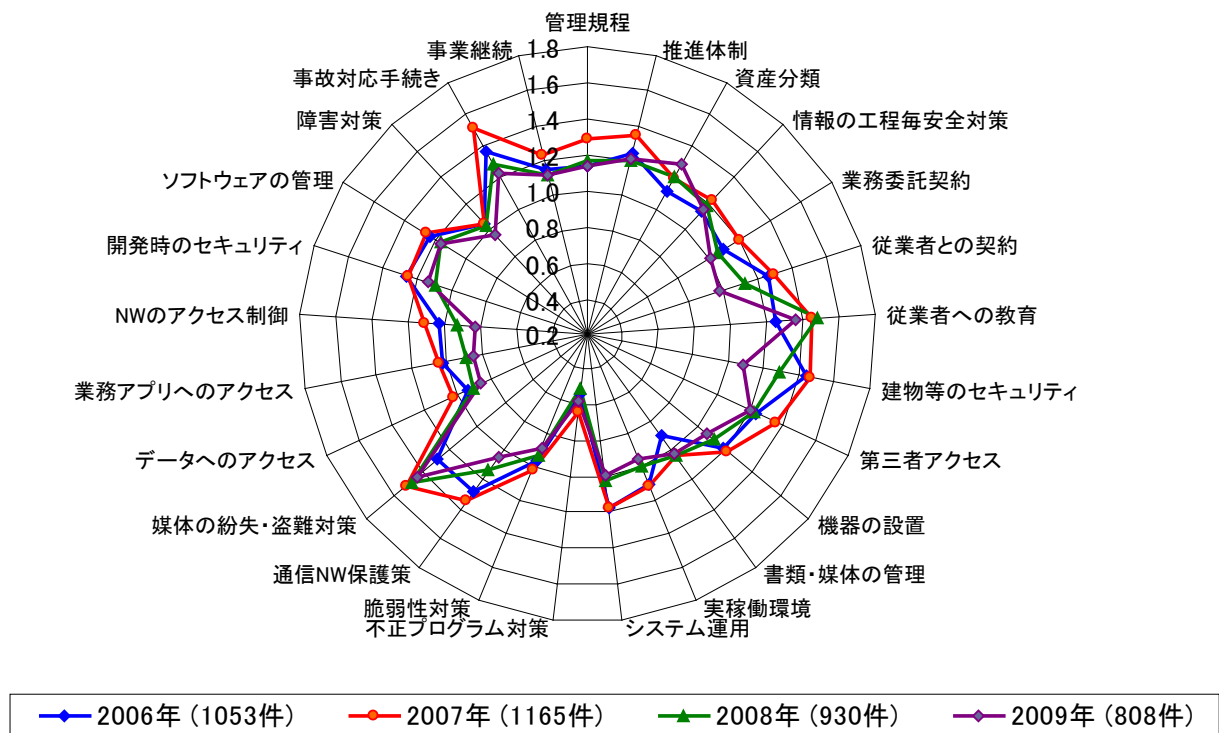


図 3 情報セキュリティ対策 25 項目スコアの分散の経年比較

情報セキュリティ対策 25 項目スコアの低い順(対策の進んでいない順番)は、2006 年、2007 年とも、「事業継続」、「開発時のセキュリティ」、「ソフトウェアの管理」の順ですが、2008 年と 2009 年では、それが、「事業継続」、「資産分類」、「ソフトウェアの管理」の順となり、資産分類に課題がシフトしていることが見て取れます。

一方、情報セキュリティ対策 25 項目スコアの分散の経年変化を見ると(図 3)、対策の進み具合にばらつきが比較的大きいのは、2007 年です。対策項目でばらつきの大きい(分散の値が大きい)順に、2006 年は、「建物等のセキュリティ」、「事故対応手続き」、「媒体の紛失・盗難対策」、2007 年は、「媒体の紛失・盗難対策」、「事故対応手続き」、「建物等のセキュリティ」、2008 年は、「従業員への教育」、「媒体の紛失・盗難対策」、「建物等のセキュリティ」、2009 年は、「媒体の紛失・盗難対策」、「従業員への教育」、「資産分類」です。

3. 中小企業の情報セキュリティ対策状況の経年比較

中小企業の各年度のトータルスコア平均を一覧を表 4 に、情報セキュリティ対策 25 項目のスコア平均の経年比較を図 4 に、トータルスコア度数分布の経年比較を図 5 に、情報セキュリティ対策 25 項目スコアの分散の経年比較を図 6 に示します。

トータルスコア平均や各評価項目スコア平均は毎年向上しています。リスク指標の平均は、毎年高くなっています。2009 年度は、トータルスコアや各項目平均の向上の度合いが他の年度よりかなり高くなっています。中小企業の対策状況の経年変化は、2. で示した全体の傾向とほぼ同様の傾向を示しています。これは、ばらつきを示す値である標準偏差や分散についても同じです。また、トータルスコアの度数分布図を見ると、2006 年度から 2008 年度は、点数の高いところから低いところへ一様にばらついているのに対し、2009 年度は、度数分布が 95 点から 100 点という点数の高い部分に多く分布し、高スコアの企業が増える傾向にあります。

2006 年と 2009 年を比べて、情報セキュリティ対策 25 項目で向上の度合いが大きい(スコアの差が大きい)項目は、順に、「従業員との契約」、「第三者アクセス」、「建物等のセキュリティ」、「開発時のセキュリティ」です。あまり変化がないのは、「不正プログラム対策」、「脆弱性対策」、「資産分類」、「障害対策」です。

表 4 中小企業の各年度のトータルスコア平均等

	トータルスコア		評価項目 スコア平均	リスク指標平均	件数
	平均	標準偏差			
2006年	69.473	19.94	2.779	-0.548	662
2007年	71.620	21.66	2.865	0.140	674
2008年	75.589	20.51	3.024	0.327	550
2009年	80.322	21.41	3.213	0.459	466

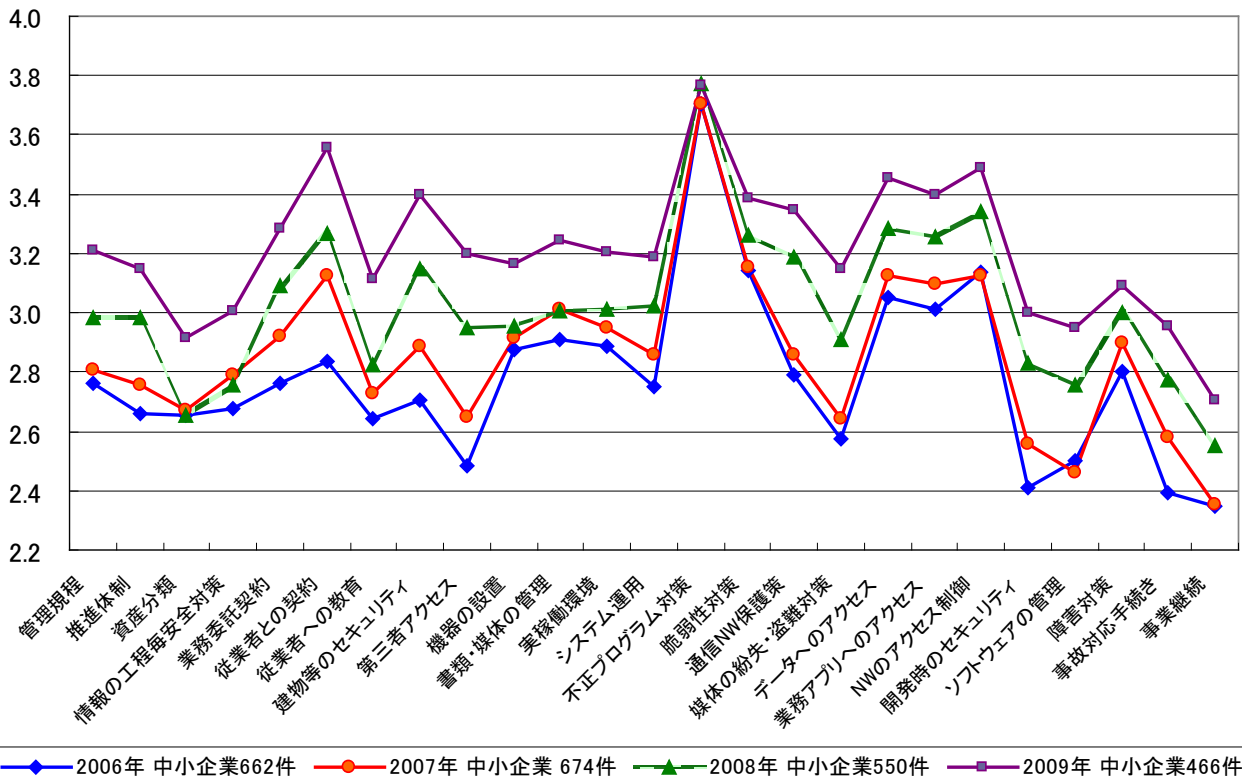


図 4 情報セキュリティ対策 25 項目のスコア平均経年比較

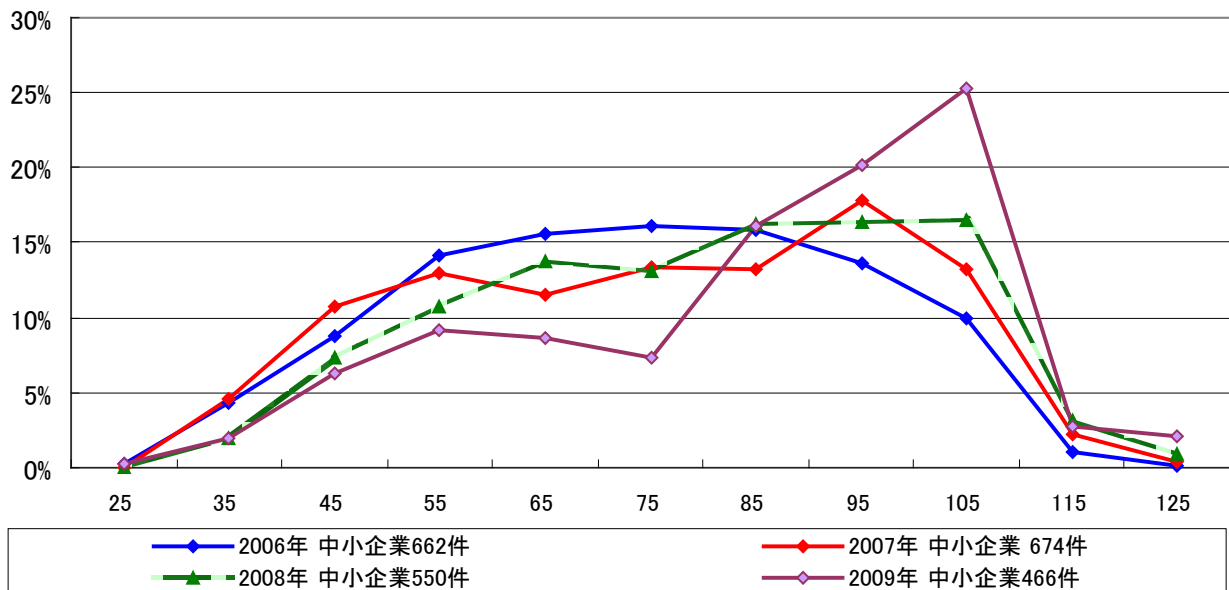


図 5 中小企業 トータルスコア度数分布の経年比較

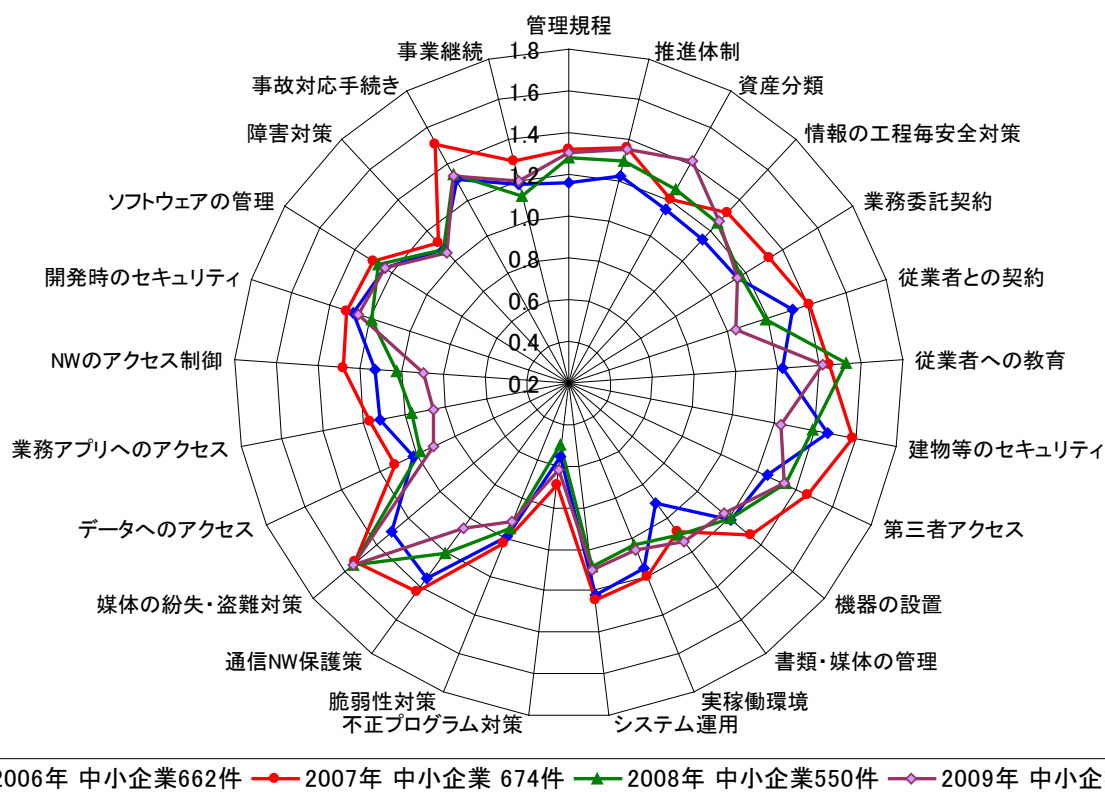


図 6 中小企業 情報セキュリティ対策 25 項目スコアの分散の経年比較

情報セキュリティ対策 25 項目スコアの低い順(対策の進んでいない順番)は、2006 年、「事業継続」、「事故対応」、「開発時のセキュリティ」の順であり、2007 年は、「事業継続」、「ソフトウェアの管理」、「開発時のセキュリティ」、2008 年および 2009 年は、「事業継続」、「資産分類」、「ソフトウェアの管理」の順です。2008 年には、資産分類が新たな課題として浮上しています。また、事業継続は経年で、どの年度でも最も対策が遅れている項目であり、資産分類や事業継続に課題があります。

一方、情報セキュリティ対策 25 項目スコアの分散の経年変化では、ばらつきの大きい(分散の値が大きい)順に、2006 年は、「建物等のセキュリティ」、「通信ネットワークの保護策」、「従業者との契約」、2007 年は、「従業者への教育」、「業務委託契約」、「脆弱性対策」、2008 年は、「媒体の紛失・盗難対策」、「従業者への教育」、「建物等のセキュリティ」、2009 年は、「媒体の紛失・盗難対策」、「従業者への教育」、「資産分類」です。2006 年には、「媒体の紛失・盗難対策」と「従業者の教育」の分散の値はそれぞれ 5 位、10 位であったものが、2008 年および 2009 年には 1 位と 2 位に浮上しており、2006 年から 2009 年にかけて、この項目で、中小企業の企業間でのばらつきが大きくなっています。

4. 大企業の情報セキュリティ対策状況の経年比較

大企業の各年度のトータルスコア平均等一覧を表 5 に、情報セキュリティ対策 25 項目のスコア平均の経年比較を図 7 に、トータルスコア度数分布の経年比較を図 8 に、情報セキュリティ対策 25 項目スコアの分散の経年比較を図 9 に示します。

表 5 大企業の各年度のトータルスコア平均等

	トータルスコア		評価項目 スコア平均	リスク指標平均	件数
	平均	標準偏差			
2006 年	79.913	17.24	3.197	0.731	391
2007 年	81.200	18.89	3.248	1.135	491
2008 年	81.689	17.97	3.268	1.445	380
2009 年	88.137	17.94	3.525	1.965	342

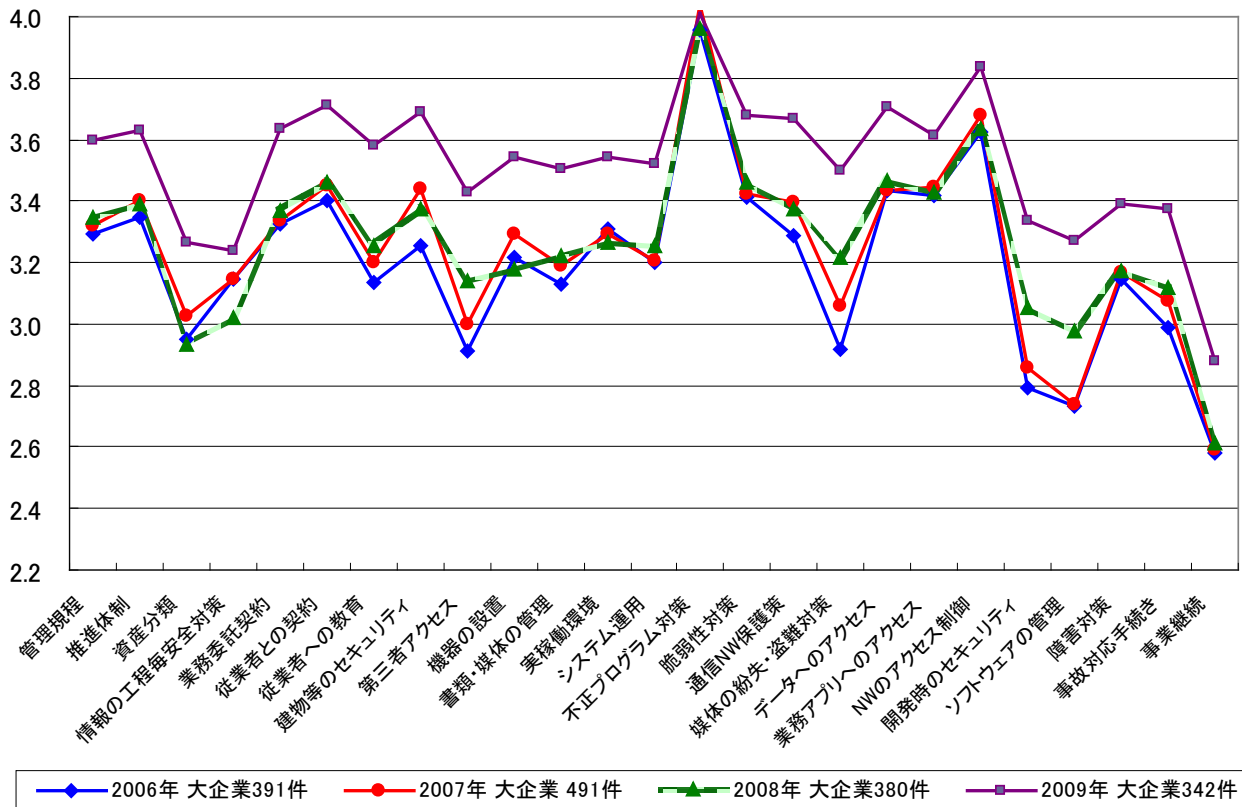


図 7 大企業 情報セキュリティ対策 25 項目のスコア平均経年比較

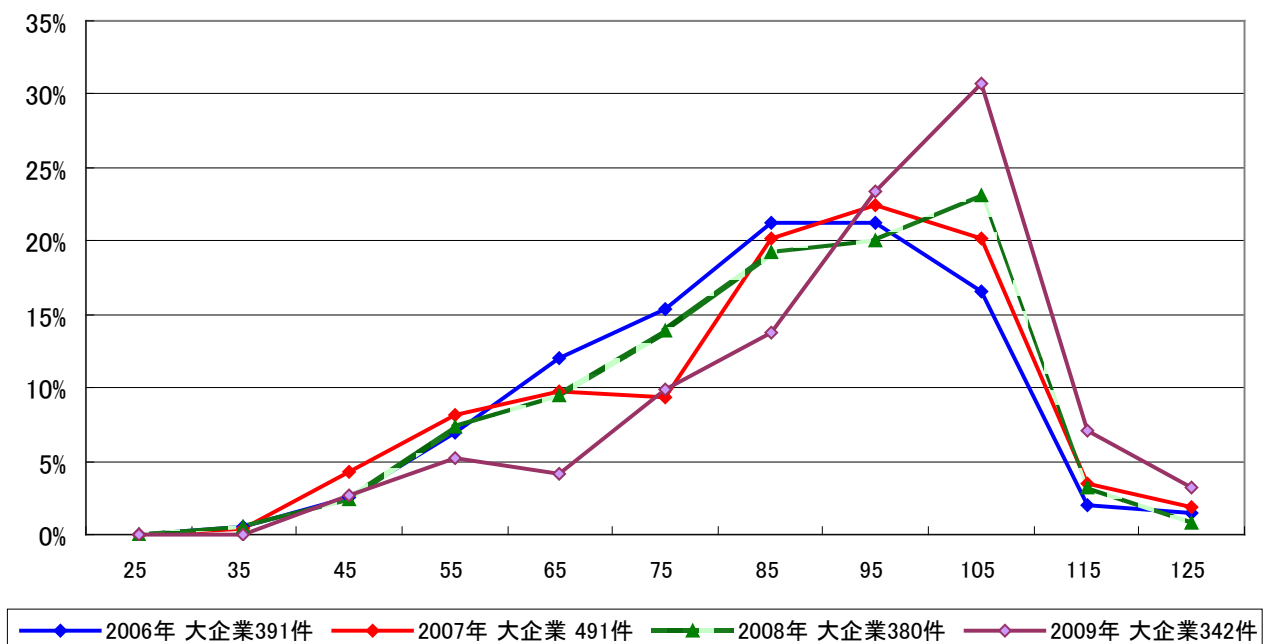


図 8 大企業 トータススコア度数分布の経年比較

トータルスコアの平均や、評価項目 25 項目のスコア平均は、2006 年から 2008 年までは毎年わずかずつ向上していたものが、2009 年には、その向上の度合いが大きくなっています。情報セキュリティリスク指標の平均も、毎年高くなっています。トータルスコアの標準偏差や情報セキュリティ対策 25 項目スコアの分散を見ると、2007 年は他の年にくらべて、わずかですが、ばらつきが大きくなっています。2006 年と 2009 年を比べて、向上の度合いが大きい(スコアの差が大きい)のは、上から順に、「媒体の紛失・盗難対策」、「開発時のセキュリティ」、「ソフトウェアの管理」、「第三者アクセス」です。

大企業はある程度対策が進んでおり、特に課題のあるところに注力しているために、経年での変化が中小企業ほどには大きくないと考えられます。また、トータルスコアの度数分布を見ると、85点から105点の間に分布する企業が多く、経年で見ると、より高いスコアの企業が増加する傾向にあります。

情報セキュリティ対策25項目のスコアの低い順(対策の進んでいない順番)は、2006年、2007年とも、「事業継続」、「ソフトウェアの管理」、「開発時のセキュリティ」、2008年は、「事業継続」、「資産分類」、「ソフトウェアの管理」、2009年は、「事業継続」、「情報の工程毎安全対策」、「資産分類」の順です。企業の大小を問わず、事業継続は対策の推進が難しい項目となっています。また、2008年には、「資産分類」が、2009年には、「情報の工程毎安全対策」が新たな課題として浮上しています。これら項目の対策がなかなか進まないのは、資産分類(情報資産の分類とラベルづけ)や情報の工程毎の安全対策の対象範囲が全社、全従業員を対象としているため、より広範囲で徹底した対応を迫られ、徹底が難しいためと考えられます。

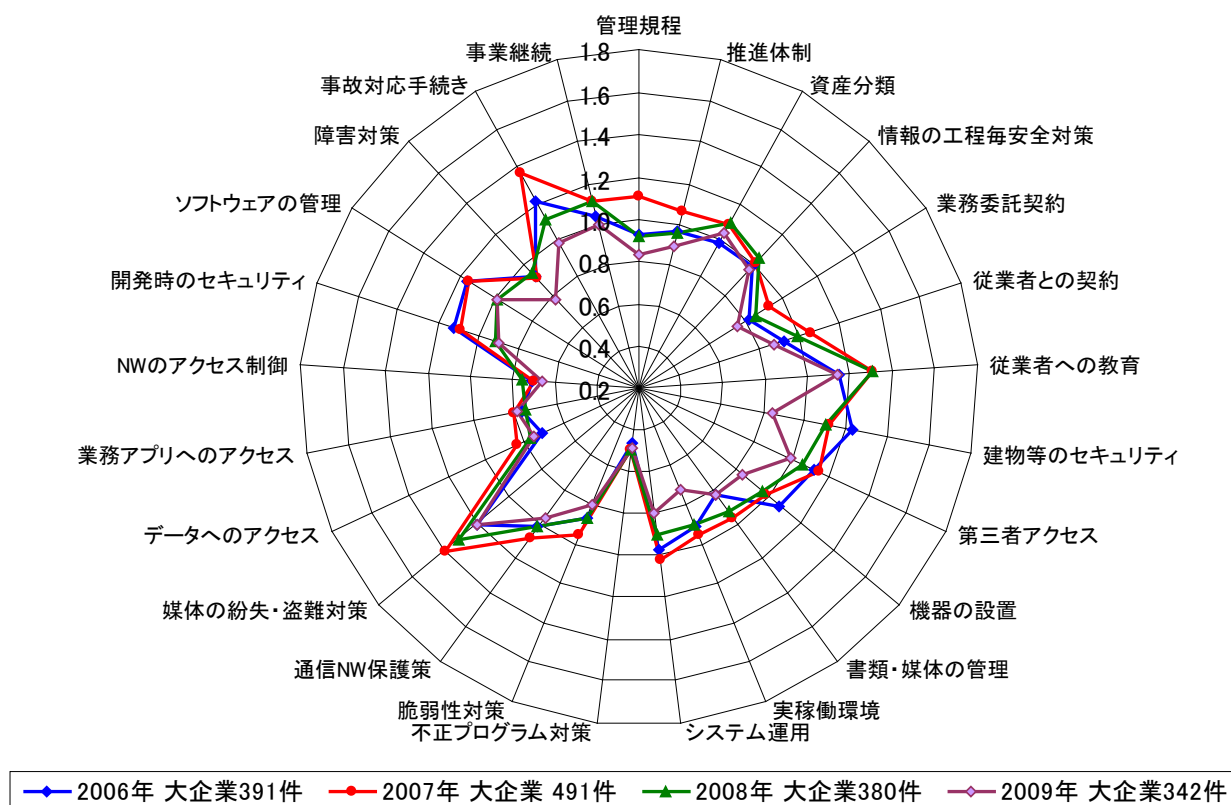


図 9 大企業 情報セキュリティ対策 25 項目スコアの分散の経年比較

情報セキュリティ対策25項目スコアの分散の経年変化については、大企業では、2006年から2008年までは、経年で大きな変化は見られなかったものの、2009年には、他の年度に比較し、大きく向上しています。また、ばらつきの大きい(分散の値が大きい)順に、2006年は、「建物等のセキュリティ」、「事故対応手続き」、「媒体の紛失・盗難対策」、2007年は、「媒体の紛失・盗難対策」、「事故対応手続き」、「従業者への教育」、2008年は、「媒体の紛失・盗難対策」、「従業者への教育」、「事故対応手続き」、2009年は、「媒体の紛失・盗難対策」、「従業者への教育」、「資産分類」です。

付録 情報セキュリティ対策項目スコア平均値等の一覧

付表1 各年度全件の情報セキュリティ対策項目スコア平均値等一覧

		2006 全体 1053 件		2007 全体 1165 件		2008 全体 930 件		2009 全体 808 件	
		平均値	分散	平均値	分散	平均値	分散	平均値	分散
	リスク指標	-0.073		0.559		0.784		1.097	
	トータルスコア	73.349		75.658		78.082		83.630	
1	管理規程	2.958	1.141	3.024	1.290	3.133	1.164	3.375	1.139
2	推進体制	2.915	1.234	3.027	1.334	3.149	1.195	3.354	1.210
3	資産分類	2.765	1.109	2.819	1.185	2.769	1.207	3.063	1.283
4	情報の工程毎安全対策	2.850	1.131	2.940	1.213	2.865	1.176	3.103	1.146
5	業務委託契約	2.972	1.100	3.096	1.199	3.205	1.053	3.432	1.009
6	従業者との契約	3.046	1.253	3.260	1.284	3.347	1.116	3.621	0.974
7	従業者への教育	2.827	1.250	2.926	1.443	3.000	1.481	3.309	1.354
8	建物等のセキュリティ	2.909	1.442	3.120	1.461	3.241	1.283	3.522	1.085
9	第三者アクセス	2.643	1.239	2.797	1.358	3.028	1.231	3.298	1.201
10	機器の設置	3.002	1.188	3.074	1.221	3.046	1.121	3.324	1.067
11	書類・媒体の管理	2.990	0.891	3.085	1.037	3.096	1.038	3.354	1.024
12	実稼働環境	3.042	1.107	3.095	1.119	3.114	0.992	3.348	0.946
13	システム運用	2.918	1.180	3.005	1.177	3.117	1.025	3.329	0.999
14	不正プログラム対策	3.799	0.534	3.845	0.632	3.851	0.502	3.869	0.573
15	脆弱性対策	3.244	0.958	3.267	1.014	3.344	0.926	3.511	0.887
16	通信 NW 保護策	2.976	1.287	3.084	1.350	3.262	1.137	3.481	1.043
17	媒体の紛失・盗難対策	2.703	1.291	2.817	1.516	3.033	1.475	3.297	1.433
18	データへのアクセス	3.196	0.939	3.255	1.025	3.360	0.900	3.562	0.854
19	業務アプリへのアクセス	3.161	1.023	3.242	1.041	3.328	0.886	3.489	0.840
20	NW のアクセス制御	3.319	1.025	3.360	1.110	3.463	0.929	3.635	0.827
21	開発時のセキュリティ	2.550	1.259	2.682	1.246	2.923	1.085	3.141	1.135
22	ソフトウェアの管理	2.588	1.222	2.578	1.254	2.846	1.170	3.085	1.159
23	障害対策	2.929	1.045	3.014	1.050	3.069	1.029	3.217	0.958
24	事故対応手続き	2.614	1.353	2.791	1.506	2.913	1.281	3.132	1.230
25	事業継続	2.434	1.141	2.455	1.229	2.578	1.114	2.777	1.118

付表2 各年度中小企業の情報セキュリティ対策項目スコア平均等一覧

		2006 中小企業 662 件		2007 中小企業 674 件		2008 中小企業 550 件		2009 中小企業 466 件	
		平均値	分散	平均値	分散	平均値	分散	平均値	分散
	リスク指標	-0.548		0.140		0.327		0.459	
	トータルスコア	69.473		71.620		75.589		80.322	
1	管理規程	2.760	1.163	2.810	1.319	2.984	1.284	3.212	1.307
2	推進体制	2.659	1.221	2.757	1.361	2.984	1.295	3.150	1.349
3	資産分類	2.656	1.149	2.669	1.208	2.656	1.261	2.916	1.414
4	情報の工程毎安全対策	2.675	1.136	2.791	1.316	2.756	1.248	3.004	1.256
5	業務委託契約	2.764	1.153	2.921	1.327	3.091	1.165	3.283	1.150
6	従業者との契約	2.834	1.325	3.123	1.410	3.269	1.192	3.556	1.043
7	従業者への教育	2.645	1.225	2.726	1.451	2.824	1.530	3.112	1.420
8	建物等のセキュリティ	2.704	1.461	2.887	1.586	3.149	1.395	3.399	1.230
9	第三者アクセス	2.485	1.249	2.647	1.465	2.951	1.340	3.202	1.336
10	機器の設置	2.875	1.217	2.914	1.336	2.955	1.209	3.165	1.175
11	書類・媒体の管理	2.908	0.913	3.010	1.083	3.009	1.098	3.242	1.143
12	実稼働環境	2.885	1.158	2.951	1.197	3.011	1.038	3.206	1.067
13	システム運用	2.752	1.227	2.859	1.245	3.024	1.091	3.187	1.103
14	不正プログラム対策	3.705	0.553	3.703	0.690	3.773	0.497	3.766	0.614
15	脆弱性対策	3.145	0.990	3.151	1.032	3.262	0.955	3.388	0.922
16	通信 NW 保護策	2.793	1.360	2.858	1.433	3.185	1.211	3.345	1.065
17	媒体の紛失・盗難対策	2.577	1.303	2.641	1.532	2.907	1.549	3.150	1.556
18	データへのアクセス	3.054	1.026	3.126	1.124	3.287	0.981	3.455	0.911

19	業務アプリへのアクセス	3.011	1.121	3.095	1.168	3.258	0.971	3.397	0.864
20	NW のアクセス制御	3.137	1.126	3.126	1.281	3.344	1.020	3.487	0.900
21	開発時のセキュリティ	2.408	1.289	2.555	1.323	2.833	1.189	2.998	1.267
22	ソフトウェアの管理	2.502	1.243	2.461	1.304	2.755	1.275	2.951	1.243
23	障害対策	2.801	1.080	2.901	1.124	2.998	1.076	3.090	1.059
24	事故対応手続き	2.393	1.310	2.582	1.513	2.771	1.346	2.955	1.333
25	事業継続	2.346	1.183	2.356	1.299	2.555	1.118	2.704	1.198

付表3 各年度大企業の情報セキュリティ対策項目スコア平均値等一覧

		2006 大企業 391 件		2007 大企業 491 件		2008 大企業 380 件		2009 大企業 342 件	
		平均値	分散	平均値	分散	平均値	分散	平均値	分散
	リスク指標	0.731		1.135		1.445		1.965	
	トータルスコア	79.913		81.200		81.689		88.137	
1	管理規程	3.294	0.926	3.318	1.103	3.350	0.914	3.596	0.828
2	推進体制	3.348	0.961	3.399	1.061	3.389	0.956	3.632	0.890
3	資産分類	2.951	0.990	3.024	1.081	2.932	1.088	3.263	1.039
4	情報の工程毎安全対策	3.146	0.986	3.145	1.001	3.021	1.034	3.237	0.967
5	業務委託契約	3.325	0.815	3.336	0.926	3.371	0.846	3.635	0.749
6	従業者との契約	3.404	0.929	3.448	1.052	3.461	0.988	3.711	0.869
7	従業者への教育	3.136	1.143	3.202	1.304	3.255	1.304	3.579	1.142
8	建物等のセキュリティ	3.256	1.222	3.440	1.116	3.374	1.095	3.690	0.842
9	第三者アクセス	2.910	1.112	3.002	1.141	3.139	1.054	3.430	0.991
10	機器の設置	3.217	1.068	3.293	0.983	3.179	0.965	3.541	0.841
11	書類・媒体の管理	3.128	0.825	3.187	0.957	3.221	0.927	3.506	0.825
12	実稼働環境	3.307	0.911	3.293	0.946	3.263	0.891	3.541	0.718
13	システム運用	3.199	0.975	3.206	1.017	3.253	0.902	3.523	0.796
14	不正プログラム対策	3.957	0.462	4.041	0.488	3.963	0.489	4.009	0.484
15	脆弱性対策	3.412	0.863	3.426	0.947	3.463	0.861	3.678	0.794
16	通信 NW 保護策	3.286	1.015	3.395	1.072	3.374	1.010	3.667	0.956
17	媒体の紛失・盗難対策	2.916	1.201	3.059	1.394	3.216	1.315	3.497	1.201
18	データへのアクセス	3.435	0.703	3.432	0.838	3.466	0.767	3.708	0.741
19	業務アプリへのアクセス	3.417	0.757	3.444	0.798	3.429	0.747	3.614	0.783
20	NW のアクセス制御	3.627	0.706	3.680	0.700	3.637	0.749	3.836	0.659
21	開発時のセキュリティ	2.790	1.120	2.855	1.091	3.053	0.910	3.336	0.892
22	ソフトウェアの管理	2.734	1.155	2.737	1.145	2.979	0.992	3.269	0.989
23	障害対策	3.146	0.915	3.169	0.908	3.171	0.944	3.389	0.772
24	事故対応手続き	2.990	1.205	3.077	1.357	3.118	1.118	3.374	0.991
25	事業継続	2.583	1.039	2.591	1.104	2.613	1.109	2.877	0.994

関連資料

- 1) 情報セキュリティ対策ベンチマーク
<http://www.ipa.go.jp/security/benchmark/>
- 2) 情報セキュリティガバナンスのページ（経済産業省）
http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html
- 3) 総務省統計局平成 18 年事業所／企業統計調査
<http://www.stat.go.jp/data/jigyoku/2006/>
- 4) 日本標準産業分類(平成 19 年 11 月改訂)
<http://www.stat.go.jp/index/seido/sangyo/19index.htm>