私立大学情報セキュリティ担当者のセキュリティ意識に関する分析

小　川　　賢

1. は　じ　め　に

大学における情報セキュリティ対策の環境は年々厳しくなっており，様々な対策が実施されている。国立大学法人は文部科学省所管の独立行政法人と同様に，政府の情報セキュリティ対策の一環として政府機関所管の独立行政法人に準じたセキュリティ対策の実施が要請されたり，国立情報学研究所の高等教育機関の情報セキュリティ対策ためのサンプル規程集の公開[4][5][8]を参考にしたりして，セキュリティポリシーの策定をはじめとした各大学でのセキュリティ対策の実施がはかられ，クラウドの利用やサイバーセキュリティ対策等時代に即した対応へと軸足を動かしつつある。

しかしながら，私立大学に対しては，私立学校の自主性の確保からもセキュリティ対策の要請も容易ではなく，私立大学情報教育協会[1][2]や大学 ICT 推進協議会の活動のほかに目立った組織的な活動も見られず，各大学の自主的な対応によるところとなっている[7]。

国立大学法人のセキュリティ対策が進む一方で，私立大学の対策が進まない現状では，私立大学の情報システムが相対的に脆弱となり攻撃の対象となりやすかったり，組織内での教育が不十分であるゆえに情報の不適切な取り扱いが起きたり等のインシデントが発生しやすくなる。

本論文では，私立大学において情報セキュリティの担当者がどのような項目を重視しているのか，所属大学のセキュリティ対策の実施過程，セキュリティポリシーの策定状況，すなわちセキュリティポリシーの策定による学内での検討を経ているかどうかで，重要視する項目に変化がみられるかどうかを検証し，セキュリティ対策を進めていくための道筋を明らかにする。

2．AHP 分析の概要

アンケートは，政府機関統一基準の管理編及び技術編の項目に関して，図１のような階層構造を有していると仮定して，それぞれの項目群の中でどの項目をどの程度重要視しているかを私立大学の情報セキュリティの担当者に質問形式で尋ねた。

項目間でどの程度重要と考えている程度に違いがあるかを調査する方法として，AHP分析による一対比較を用いることが多いが，一対比較形式で質問した場合，回答数が膨大になり回答者の負担となり，回収率に影響を及ぼすことを考慮し，特定の群の中で重要と思う項目に対して持点を配分することで持ち分配点法によるアンケートを行った。

調査は，2011年12月９日に全国の私立大学594校に送付し117校より回答があり，回収率は19.7％であった。

各項目の重要度の認識調査と合わせて質問したセキュリティポリシーの策定状況については，策定状況を回答した大学113校のうち，策定済が52校（46％），策定中が30校（26.5％），策定していないが27校（23.9％），現在検討中や審議中等が４校であった。

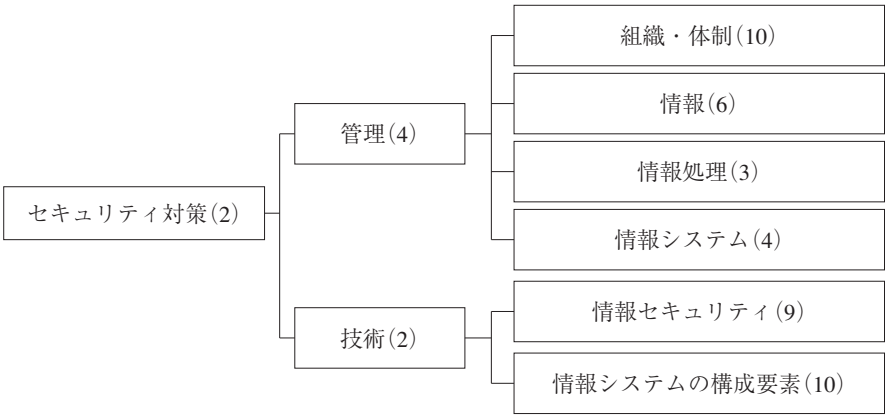

図１　セキュリティ対策の項目の階層構造

2.1．管理に関するアンケート項目

ここでは実施したアンケートの回答内容のうち，管理に関する項目について回答の概要を述べていく。

2.1.1．管理に関する項目群について

管理面全体の項目間の重要度について質問した。４項目の合計が100点となるように配

点してもらった。項目への最大配点は求めなかった。

回答者が 4 項目に何点を付けたかをまとめたものが表 1 である。

表 1　管理に関する対策についての集計結果

	0	20	40	60	70
1 組織・体制の整備を行うこと	0	18	80	13	2
2 情報システムについての対策を行うこと	2	54	55	2	0
3 情報処理についての対策を行うこと	2	78	32	1	0
4 情報についての基本的な対策を行うこと	0	42	67	4	0

2.1.2. 組織と体制の整備について

組織と体制の整備については次の10項目の合計が100点となるように，重要と思われる項目に配点してもらう形で，回答してもらった。項目間での関係をみるために，配点は 5 項目以上，最も重要視する項目への最大配点は20点，という条件を付けた。

回答者が10項目に何点を付けたかをまとめたものが表 2 である。

表 2　組織と体制の整備についての集計結果

	0	5	10	15	20
1 各責任者や委員会等を設置し組織・体制を定めること	2	5	18	8	80
2 兼務が禁止される場合や上司による承認・許可等役割の割り当てを定めること	62	25	18	2	6
3 違反への対処や例外措置について定めること	31	26	39	9	8
4 情報セキュリティ対策の教育の実施について定めること	4	7	37	33	32
5 障害・事故等への事前準備，対処，原因調査と再発防止策について定めること	10	0	36	28	39
6 情報セキュリティ対策の自己点検について定めること	12	18	53	24	6
7 情報セキュリティ対策の監査について定めること	22	19	47	15	10
8 情報セキュリティ対策の見直しについて定めること	22	16	48	15	12
9 委託先への要求事項など外部委託について定めること	33	26	33	12	9
10事業継続計画と情報セキュリティ対策の整合的運用の確保について定めること	21	15	47	16	14

2.1.3. 情報システムの基本的な対策について

情報システムの基本的な対策については次の 9 項目の合計が100点となるように，重要と思われる項目に配点してもらう形で，回答してもらった。項目間での関係をみるために付けた条件は組織と体制の整備についての質問と同様である。

回答者が９項目に何点を付けたかをまとめたものが表３である。

表３　情報システムの基本的な対策についての集計結果

	0	5	10	15	20
１情報システムのライフサイクルに応じたセキュリティ要件について遵守事項を定めること	7	3	36	22	41
２情報システムに係る文書及び台帳整備についての規定の整備と遵守事項を定めること	5	5	33	30	36
３機器等の購入についての規定の整備と遵守事項を定めること	21	18	38	16	16
４ソフトウェア開発についての規定の整備と遵守事項を定めること	48	21	23	7	10
５主体認証・アクセス制御，権限管理等についての規定の整備と遵守事項を定めること	8	1	17	25	58
６暗号と電子署名についての規定の整備と遵守事項を定めること	30	10	47	15	7
７学外の情報セキュリティ水準の低下を招く行為の防止についての規定の整備と遵守事項を定めること	15	7	26	31	30
８ドメイン名の使用についての規定の整備と遵守事項を定めること	38	25	32	10	4
９不正プログラム感染防止についての規定の整備と遵守事項を定めること	2	5	36	29	37

2.1.4. 情報処理に関する対策について

情報処理に関する対策については次の３項目の合計が100点となるように，重要と思われる項目に配点してもらう形で，回答してもらった。

回答者が３項目に何点を付けたかをまとめたものが表４である。

表４　情報処理に関する対策についての集計結果

	0	20	40	60	80
１情報処理に関する対策として情報システムの利用についての遵守事項を定めること	1	5	44	54	12
２情報処理に関する対策として学外での情報処理の制限についての遵守事項を定めること	6	49	59	2	0
３情報処理に関する対策として持込機器による情報処理の制限についての遵守事項を定めること	0	25	80	11	0

2.1.5. 情報に関する対策について

情報に関する対策については次の６項目の合計が100点となるように，４項目以上に配

点し，最も重要視する項目への最大配点は20点という条件を付けた。

回答者が 6 項目に何点を付けたかをまとめたものが表 5 である。

表 5　情報に関する対策についての集計結果

	0	5	10	15	20
1 情報に関する対策として情報の作成と入手についての遵守事項を定めること	5	1	18	24	64
2 情報に関する対策として情報の利用についての遵守事項を定めること	0	0	6	18	88
3 情報に関する対策として情報の保存についての遵守事項を定めること	1	0	14	25	72
4 情報に関する対策として情報の移送についての遵守事項を定めること	5	1	24	35	48
5 情報に関する対策として情報の提供についての遵守事項を定めること	1	1	20	17	73
6 情報に関する対策として情報の消去についての遵守事項を定めること	4	0	26	27	55

2.2. 技術に関するアンケート項目

ここでは実施したアンケートの回答内容のうち，管理に関する項目について分析結果を述べていく。

2.2.1. 情報セキュリティに関する要件について

情報セキュリティに関する要件については次の 9 項目の合計が100点となるように，5 項目以上に配点し，最も重要視する項目への最大配点は20点という条件を付けた。

回答者が 9 項目に何点を付けたかをまとめたものが表 6 である。

表 6　情報セキュリティに関する要件についての集計結果

	0	5	10	15	20
1 機能としての主体認証に関する要件を明確にすること	22	5	29	20	35
2 機能としてのアクセス制御に関する要件を明確にすること	1	2	34	28	46
3 機能としての権限管理に関する要件を明確にすること	4	0	26	33	48
4 機能としての証跡管理に関する要件を明確にすること	12	13	34	26	26
5 機能としての暗号と電子署名に関する要件を明確にすること	36	14	49	8	4
6 脅威としてのセキュリティホール対策に関する要件を明確にすること	12	13	45	23	18

7 脅威としての不正プログラム対策に関する要件を明確にすること	4	18	51	19	19
8 脅威としてのサービス不能攻撃対策に関する要件を明確にすること	26	28	37	12	8
9 情報セキュリティの脅威として踏み台対策に関する要件を明確にすること	20	22	44	13	12

2.2.2. 情報システムの構成要素に関する要件について

情報システムの構成要素に関する要件については次の10項目の合計が100点となるように，５項目以上に配点し，最も重要視する項目への最大配点は20点という条件を付けた。

回答者が10項目に何点を付けたかをまとめたものが表７である。

表７　情報システムの構成要素に関する集計結果

	0	5	10	15	20
1 情報システムを設置する安全区域に関する要件を明確にすること	26	10	36	10	32
2 電子計算機共通の設置時，運用時及び運用終了時に関わる要件を明確にすること	38	19	35	8	14
3 端末の設置時，運用時及び運用終了時に関わる要件を明確にすること	19	15	49	15	16
4 サーバ装置の設置時，運用時及び運用終了時に関わる要件を明確にすること	4	7	45	28	30
5 電子メールの導入時及び運用時に関わる要件を明確にすること	12	6	47	25	24
6 ウェブサーバの導入時及び運用時に関わる要件を明確にすること	7	9	56	22	20
7 DNS の導入時及び運用時に関わる要件を明確にすること	22	16	47	14	15
8 通信回線の構築時，運用時及び運用終了時に関わる要件を明確にすること	33	20	47	6	8
9 学内回線の構築時及び運用時，回線の対策に関わる要件を明確にすること	18	21	45	16	14
10学内回線と学外回線との接続時及び運用時に関わる要件を明確にすること	19	14	49	15	17

2.2.3. 技術に関する対策について

技術面全体の項目間の重要度について質問した。２項目の合計が100点となるように配点してもらった。項目への最大配点は求めなかった。

回答者が２項目に何点を付けたかをまとめたものが表８である。

表8　技術に関する対策についての集計結果

	20	30	40	50	60	70	80
1情報セキュリティに関する要件について	1	1	9	44	40	15	6
2情報システムの構成要素に関する要件について	6	15	40	43	10	1	1

2.3. 重要度の計算

これらを図1のような階層構造とみなし，項目間の重要度を掛け合わせることで第4階層までの項目それぞれの重要度を表9及び10のように計算した。

表9　計算された管理に関する項目の重要度

	平均	標準偏差	中央値
管理面に関する質問内容	0.5527	0.125655	0.5
組織・体制の整備を行うこと	0.1785	0.108356	0.15
各責任者や委員会等を設置し組織・体制を定めること	0.0318	0.02357	0.029
兼務が禁止される場合や上司による承認・許可等役割の割り当てを定めること	0.0096	0.022742	0.0
違反への対処や例外措置について定めること	0.0127	0.012068	0.0105
情報セキュリティ対策の教育の実施について定めること	0.0233	0.015872	0.0205
障害・事故等への事前準備，対処，原因調査と再発防止策について定めること	0.0236	0.021331	0.021
情報セキュリティ対策の自己点検について定めること	0.0159	0.013173	0.0138
情報セキュリティ対策の監査について定めること	0.0146	0.013424	0.0113
情報セキュリティ対策の見直しについて定めること	0.0151	0.015023	0.0125
委託先への要求事項など外部委託について定めること	0.0155	0.022624	0.0103
事業継続計画と情報セキュリティ対策の整合的運用の確保について定めること	0.0165	0.015091	0.015
情報についての対策を行うこと	0.1274	0.062157	0.125
情報に関する対策として情報の作成と入手についての遵守事項を定めること	0.0221	0.013336	0.02
情報に関する対策として情報の利用についての遵守事項を定めること	0.0235	0.012344	0.0225
情報に関する対策として情報の保存についての遵守事項を定めること	0.0215	0.010418	0.02
情報に関する対策として情報の移送についての遵守事項を定めること	0.0187	0.011864	0.0184
情報に関する対策として情報の提供についての遵守事項を定めること	0.0215	0.011412	0.0207
情報に関する対策として情報の消去についての遵守事項を定めること	0.0201	0.012586	0.018
情報処理についての対策を行うこと	0.1026	0.045889	0.1
情報処理に関する対策として情報システムの利用についての遵守事項	0.0471	0.025099	0.0465
情報処理に関する対策として学外での情報処理の制限についての遵守事項	0.0237	0.015315	0.024
情報処理に関する対策として持込機器による情報処理の制限についての遵守事項	0.0318	0.017754	0.03
情報システムについての基本的な対策を行うこと	0.1443	0.079713	0.14
情報システムのライフサイクルに応じたセキュリティ要件についての遵守事項	0.0201	0.015902	0.018
情報システムに係る文書及び台帳整備についての規定の整備と遵守事項	0.0212	0.017238	0.018
機器等の購入についての規定の整備と遵守事項	0.0135	0.011915	0.0125
ソフトウェア開発についての規定の整備と遵守事項	0.0083	0.010879	0.004
主体認証・アクセス制御，権限管理等についての規定の整備と遵守事項	0.023	0.017518	0.02

暗号と電子署名についての規定の整備と遵守事項	0.0124	0.015842	0.0095
学外の情報セキュリティ水準の低下を招く行為の防止について	0.0164	0.010972	0.016
ドメイン名の使用についての規定の整備と遵守事項	0.0078	0.008038	0.0061
不正プログラム感染防止についての規定の整備と遵守事項を定めること	0.0216	0.016156	0.0188

表10　計算された技術に関する項目の重要度

	平均	標準偏差	中央値
技術面に関する質問内容	0.4473	0.125655	0.5
情報セキュリティに関する要件について	0.2446	0.06873	0.25
機能としての主体認証に関する要件を明確にすること	0.0285	0.020022	0.026
機能としてのアクセス制御に関する要件を明確にすること	0.0371	0.014001	0.0375
機能としての権限管理に関する要件を明確にすること	0.038	0.0153	0.0368
機能としての証跡管理に関する要件を明確にすること	0.0281	0.017279	0.025
機能としての暗号と電子署名に関する要件を明確にすること	0.0169	0.014641	0.02
脅威としてのセキュリティホール対策に関する要件を明確にすること	0.0283	0.017816	0.025
脅威としての不正プログラム対策に関する要件を明確にすること	0.0275	0.015121	0.025
脅威としてのサービス不能攻撃対策に関する要件を明確にすること	0.0186	0.015465	0.017
情報セキュリティの脅威として踏み台対策に関する要件を明確にすること	0.0217	0.016275	0.0205
情報システムの構成要素に関する要件について	0.2027	0.088757	0.2
情報システムを設置する安全区域に関する要件を明確にすること	0.0208	0.016514	0.02
電子計算機共通の設置時，運用時及び運用終了時に関わる要件を明確にすること	0.016	0.018823	0.0125
端末の設置時，運用時及び運用終了時に関わる要件を明確にすること	0.0196	0.014165	0.018
サーバ装置の設置時，運用時及び運用終了時に関わる要件を明確にすること	0.026	0.017494	0.024
電子メールの導入時及び運用時に関わる要件を明確にすること	0.023	0.01827	0.022
ウェブサーバの導入時及び運用時に関わる要件を明確にすること	0.0247	0.019269	0.024
DNS の導入時及び運用時に関わる要件を明確にすること	0.018	0.015567	0.016
通信回線の構築時，運用時及び運用終了時に関わる要件を明確にすること	0.0161	0.01414	0.016
学内回線の構築時及び運用時，回線の対策に関わる要件を明確にすること	0.0179	0.013683	0.016
学内回線と学外回線との接続時及び運用時に関わる要件を明確にすること	0.0205	0.016326	0.019

2.3.1. 第１階層からみた第２階層

セキュリティ対策という観点から，管理的要素と技術的要素との比較では，回答者全体の平均値を見ると，配分の比では55.2％と44.7％とやや管理的要素を重視する回答が多くなっている。標準偏差も0.126と同じであるが，管理的要素の最大値は100％で最小値は20％である一方で，技術的要素の最大値は80％で最小値は０％とやや全体的に管理的要素を重要視している傾向が見て取れる。これは，多くの大学において，一部または多くの情報システムの運用・管理で，外部業者への委託を行っていることから，大学の情報システム管理部門のスタッフが技術的対応を行うことよりも，全学的な管理に業務の重きが置かれ

ていることによると考えるのが妥当であろう。

2.3.2. 第2階層からみた第3階層

管理的要因からみた，組織・体制に関する項目，情報ついての対策に関する項目，情報処理についての対策に関する項目，情報システムに関する項目の比較についてみていく。回答者全体の平均値は，組織・体制に関する項目については17.9%，情報システムに関する項目については14.4%，情報ついての対策に関する項目については12.7%，情報処理についての対策に関する項目については10.3%となった。これら4つの項目の中では，組織・体制の整備を重要視する回答が多く，次に情報システムについての対策を重視する回答が多かった。それぞれの積み上げた重要度を見ても，組織・体制の整備の中央値は15.0%，情報システムに関する項目が14.0%，情報に関する項目が12.5%，情報処理に関する項目が10.0%となっている。組織・体制の整備は，この項目に大きく配分した回答が含まれるため，他の3項目に比して中央値よりも平均が高くなっている。これは，標準偏差を見ても，他の3項目は4.6%から8.0%であるが，10.8%と大きくなっていることからもやや，ばらつきが見られる。

次に，技術的要因からみた，情報セキュリティに関する項目，情報システムの構成要素に関する項目の比較についてみていく。

情報セキュリティに関する要件については全体の平均が24.5%と2つ目の階層の6項目の中では最も高く，情報システムの構成要素については，全体の平均が20.3%と2つ目の階層の6項目の中で2番目に高く，どちらも中央値と平均値の差は小さく，標準偏差も6.9と8.9と低く，ほとんどの回答者がこの2つの要素については重要であると考えている。

2.3.3. 第3階層から見た第4階層

組織・体制の整備を行う項目からみた，その下の10項目についてみていく。10項目は導入，運用，評価，見直し，その他に分類される。導入には，各責任者や委員会等を設置し組織・体制を定めること，兼務が禁止される場合や上司による承認・許可等役割の割り当てを定めること，違反への対処や例外措置について定めること，が含まれる。運用には情報セキュリティ対策の教育の実施について定めること，障害・事故等への事前準備，対処，原因調査と再発防止策について定めること，が含まれる。評価には，情報セキュリティ対策の自己点検について定めること，情報セキュリティ対策の監査について定めること，が含まれる。見直しには，情報セキュリティ対策の見直しについて定めること，委託先への要求事項など外部委託について定めること，が含まれる。その他には，事業継続計画と情

報セキュリティ対策の整合的運用の確保について定めること，が含まれる。組織・体制の整備の項目の中では，責任者や委員会を設置し組織・体制を定めることの割合が3.2％と高く，次いで障害・事故への事前対応の2.36％，情報セキュリティ対策の教育の実施の2.3％あたりが目立つ。やはり，東日本大震災による情報システムへの影響がこのアンケートにも出ている。自然災害などの非常事態への対応として，通常時のみならず非常時の組織・体制を整備し，非常事態が発生した場合の想定される対応の整備，非常時の情報伝達や対応について利用者に周知徹底すること，これらの項目は非常時に迅速な対応を行うためには特に重要な項目である。

情報についての対策項目から見た，その下の６項目についてみていく。情報の作成と入手，情報の利用，情報の保存，情報の移送，情報の提供，情報の消去であるが，情報の移送のみがやや小さく1.9％であったが，そのほかの５項目は，すべて２％前半であった。中央値との差もほとんどなく，６項目をほぼ同程度に重要と考えている。

情報処理についての対策に関する項目から見た，３項目についてみていく。情報システムの利用についての遵守事項を定めること，学外での情報処理の制限についての遵守事項を定めること，持込機器による情報処理の制限についての遵守事項であるが，情報システムの利用についての遵守事項を定めることが4.7％と第４階層の項目としては高く重要であると評価されている。これは，情報システムの利用に関する規定として各大学で制定されている規則との関係からこの項目への意識が高くなったといえる。次に持込機器による情報処理の制限についての遵守事項を定めることが3.2％と高い。学外での情報処理の制限については，前２項目と比較すれば重要ではないが，第４階層全体から見れば，ほぼ平均的な重要度と評価されている。大学の場合，教員や学生による私物パソコンやタブレット，スマートフォンによる学内システムへの接続や利用が日常的に行われている。また，教員は学外でも，私物パソコンや持ち出した備品のノートパソコンで情報処理を行っているため，制限についての遵守事項を定めることが重要であるとの意識は高いが，利便性とセキュリティのバランスをどのレベルで取るかそれぞれの大学の組織の考え方や教職員の意識のばらつき等で実施は容易ではないことから重要と評価されている。

情報システムについての基本的な対策を行うことから見た，その下の９項目についてみていく。９項目は，情報システムのライフサイクルと，情報システムに係る文書及び台帳整備，機器等の購入について，ソフトウェア開発，主体認証・アクセス制御，権限管理等について，暗号と電子署名について，学外の情報セキュリティ水準の低下を招く行為の防止について，ドメイン名の使用について，不正プログラム感染防止について，の規定の整備に分けられる。９項目のうち，ソフトウェア開発，ドメイン名の使用についての２項目

は重要度がそれほど高くなかった。自組織で業務用のソフトウェアの開発を行っている大学が少ないこと，ドメイン名の管理について，一括管理がなされていて影響が軽微であると判断されたことが，重要度が高くない要因と考えられる。主体認証・アクセス制御，権限管理等について，不正プログラム感染防止について，情報システムに係る文書及び台帳整備については，全体から見てほぼ平均的な重要度と評価されている。

情報セキュリティに関する要件から見たその下の 9 項目についてみていく。9 項目は，主体認証に関する要件，アクセス制御に関する要件，権限管理に関する要件，証跡管理に関する要件，暗号と電子署名に関する要件，のセキュリティの機能としての対応項目と，セキュリティホール対策に関する要件，不正プログラム対策に関する要件，サービス不能攻撃対策に関する要件，踏み台対策に関する要件，のセキュリティの脅威への対応項目に分けられる。重要度の値では，権限管理に関する要件とアクセス制御に関する要件が3.8％と3.7％と第 4 階層の中でも一番目と二番目に高い。セキュリティの機能としての対応項目は，暗号と電子署名に関する項目以外概ね重要視されている。暗号と電子署名については，通常の大学の情報システムの運用では項目として必要とされることが少なく，暗号化や電子署名が必要との判断に至る例が少ないことがこの項目の重要度が高くない理由であろう。セキュリティの脅威への対応項目では，セキュリティホールや不正プログラム対策の値が高く評価されている。ほかの項目よりも具体的なイメージと対策の重要性を組織内で説明しやすいことが要因として考えられる。

情報システムの構成要素に関する要件から見た，その下の10項目についてみていく。この10項目は，情報システムを設置する安全区域と，電子計算機共通・端末・サーバ装置の設置時・運用時及び運用終了時に関わる要件の電子計算機に関わる要件，電子メール・ウェブサーバ・DNS の導入時・運用時及び運用終了時に関わる要件，のアプリケーションに関わる要件，通信回線共通の対応，学内回線の管理，学外回線の接続，の通信回線に関する項目の 4 つに分類される。10項目の中で重要視されているのは，安全区域に関する要件，サーバ装置と電子メール，ウェブサーバに関する要件，学外回線との接続の 5 項目である。サーバ装置，電子メールシステム，ウェブサーバについては，不正アクセスやアクセス権限の設定ミスで関係者以外が閲覧可能ではない情報が閲覧可能になっていたインシデント等が発生していたため，重要度が高まったと考えられる。

技術面に分類される第 4 層の項目は管理面に分類される第 4 層の項目よりもおおむね重要であると評価されている。大学の組織の中で，規則を制定して情報セキュリティ体制を構築し各部局に PDCA サイクルの実施を周知徹底することと，情報システムの管理部署で検討・決定できる対策事項であれば，迅速性と合意形成の容易さから管理部署内で対応

できる範囲から進めていくことが一般的であるためこのような傾向が得られたのであろう。

3．所属大学のポリシー策定状況別の考察

前章では，セキュリティ対策項目へのAHPによる重要度の配分について考察したが，アンケートでは，所属大学のセキュリティポリシーの策定状況についても質問しており，この章では，回答者の項目への配点割合が，所属大学のセキュリティポリシーの策定状況が重要度の配分によって異なるかどうかを考察していく。セキュリティポリシーの策定状況別に各項目の平均値，標準偏差，中央値をまとめたものが表11及び12である。

表11　所属大学の策定状況別された管理に関する項目の重要度の概要

	策定済			策定中			未策定		
	Ave	SE	Med	Ave	SE	Med	Ave	SE	Med
管理面に関する質問内容	0.522	0.123	0.5	0.558	0.129	0.5	0.6	0.115	0.6
組織・体制の整備	0.174	0.069	0.15	0.191	0.158	0.15	0.168	0.078	0.163
組織・体制	0.03	0.016	0.028	0.034	0.034	0.025	0.031	0.018	0.033
役割の割り当て	0.008	0.013	0.0	0.014	0.036	0.005	0.006	0.009	0.0
違反への対処や例外措	0.013	0.013	0.01	0.009	0.009	0.009	0.017	0.013	0.015
教育の実施	0.025	0.011	0.023	0.022	0.018	0.019	0.023	0.02	0.017
障害・事故等	0.022	0.015	0.023	0.027	0.031	0.02	0.022	0.013	0.021
自己点検	0.016	0.01	0.015	0.017	0.018	0.013	0.013	0.01	0.013
監査	0.016	0.012	0.014	0.014	0.013	0.01	0.013	0.016	0.01
見直し	0.016	0.016	0.013	0.017	0.017	0.014	0.011	0.01	0.01
外部委託	0.013	0.011	0.01	0.021	0.035	0.01	0.013	0.011	0.012
事業継続計画	0.015	0.013	0.015	0.017	0.017	0.018	0.019	0.016	0.014
情報についての対策を行うこと	0.119	0.053	0.12	0.111	0.055	0.125	0.165	0.073	0.15
情報の作成と入手	0.021	0.011	0.02	0.017	0.009	0.019	0.031	0.017	0.029
情報の利用	0.022	0.011	0.02	0.021	0.011	0.023	0.031	0.015	0.03
情報の保存	0.02	0.01	0.019	0.02	0.01	0.02	0.027	0.01	0.03
情報の移送	0.019	0.009	0.018	0.017	0.011	0.017	0.021	0.017	0.019
情報の提供	0.02	0.011	0.02	0.02	0.011	0.024	0.026	0.012	0.023
情報の消去	0.018	0.011	0.016	0.017	0.01	0.018	0.029	0.015	0.026
情報処理について	0.092	0.039	0.1	0.103	0.052	0.1	0.121	0.044	0.12
情報システムの利用	0.04	0.018	0.04	0.046	0.026	0.045	0.062	0.028	0.06
学外での情報処理	0.025	0.016	0.026	0.023	0.014	0.023	0.023	0.017	0.02
持込機器	0.027	0.014	0.03	0.034	0.021	0.031	0.036	0.017	0.036
情報システムについて	0.137	0.084	0.125	0.152	0.09	0.125	0.146	0.056	0.145
ライフサイクル	0.019	0.015	0.018	0.022	0.02	0.018	0.02	0.01	0.018

文書及び台帳整備	0.018	0.019	0.015	0.022	0.018	0.019	0.024	0.012	0.023
機器等の購入	0.013	0.013	0.012	0.014	0.01	0.015	0.014	0.013	0.013
ソフトウェア開発	0.007	0.009	0.005	0.01	0.013	0.006	0.007	0.01	0.0
権限管理等	0.024	0.017	0.02	0.023	0.021	0.018	0.022	0.012	0.022
暗号と電子署名	0.012	0.016	0.008	0.013	0.018	0.012	0.011	0.013	0.008
情報セキュリティ水準	0.017	0.011	0.015	0.014	0.011	0.013	0.019	0.011	0.02
ドメイン名の使用	0.007	0.007	0.005	0.009	0.009	0.008	0.007	0.008	0.008
不正プログラム	0.02	0.017	0.018	0.024	0.018	0.02	0.021	0.011	0.018

表12　所属大学の策定状況別された技術に関する項目の重要度の概要

	策定済			策定中			未策定		
	Ave	SE	Med	Ave	SE	Med	Ave	SE	Med
技術面に関する質問内容	0.478	0.123	0.5	0.442	0.129	0.5	0.4	0.115	0.4
情報セキュリティに関する要件	0.254	0.067	0.25	0.247	0.077	0.25	0.225	0.057	0.24
主体認証	0.029	0.022	0.025	0.032	0.019	0.036	0.022	0.018	0.025
アクセス制御	0.038	0.015	0.036	0.035	0.014	0.036	0.039	0.013	0.039
権限管理	0.039	0.017	0.042	0.039	0.015	0.038	0.035	0.011	0.036
証跡管理	0.026	0.018	0.025	0.031	0.017	0.03	0.028	0.015	0.026
暗号と電子署名	0.017	0.014	0.016	0.017	0.016	0.024	0.017	0.015	0.019
セキュリティホール対策	0.031	0.019	0.028	0.029	0.018	0.03	0.023	0.015	0.024
不正プログラム対策	0.028	0.016	0.025	0.028	0.017	0.028	0.025	0.012	0.024
サービス不能攻撃対策	0.022	0.017	0.018	0.017	0.014	0.016	0.016	0.014	0.014
踏み台対策	0.025	0.019	0.024	0.019	0.013	0.018	0.02	0.013	0.021
情報システムの構成要素	0.224	0.102	0.2	0.195	0.073	0.2	0.175	0.076	0.16
安全区域	0.023	0.017	0.025	0.021	0.017	0.02	0.017	0.015	0.012
電子計算機共通	0.02	0.023	0.016	0.015	0.016	0.012	0.011	0.011	0.009
端末	0.019	0.014	0.016	0.022	0.016	0.02	0.018	0.011	0.018
サーバ装置	0.029	0.021	0.025	0.024	0.014	0.024	0.024	0.015	0.024
電子メール	0.026	0.022	0.025	0.019	0.014	0.02	0.023	0.016	0.02
ウェブサーバ	0.027	0.024	0.024	0.022	0.014	0.024	0.023	0.015	0.022
DNS	0.022	0.018	0.02	0.016	0.011	0.018	0.014	0.016	0.013
通信回線	0.02	0.016	0.016	0.014	0.012	0.016	0.012	0.012	0.012
学内回線	0.018	0.013	0.015	0.02	0.015	0.02	0.016	0.012	0.013
学外回線との接続	0.021	0.019	0.018	0.022	0.015	0.023	0.018	0.014	0.016

3.1. 第１階層から見た第２階層

管理的要素と技術的要素の配点状況を見ていくと，策定済の大学の回答者の回答の平均

値は管理的要素が52.2％で技術的要素が47.8％であるのに対し，策定中の大学の回答者の回答の平均値は管理的要素が55.8％で技術的要素が44.2％，未策定の大学の回答者の回答の平均値は管理的要素が60.0％で技術的要素が40.0％と，セキュリティポリシーの策定が進むにつれて，管理面よりも技術的な項目に重きを置くようになっている。これは，ポリシー策定で，組織・体制の整備が一通り完了し具体的な技術的対応にシフトしていっていることがうかがえる。中央値と平均値の差もほとんどなく，配分のばらつきは小さい。

3.2. 第２階層から見た第３階層

管理的要素から見た組織・体制の整備に関しては，策定状況が進むにつれて管理面の割合が低くなっていくが，策定済の平均値が17.5％，策定中の平均値が19.1％，未策定の平均値が16.8％となっている。中央値は策定済と策定中が15.0％，未策定が16.3％となっている。策定中の平均値が高くなった要因はセキュリティポリシーの策定途中で組織や体制をどのようにするかを検討しているため，重要と判断した回答があったため上に振れたことが考えられる。策定済においても未策定の大学においても，組織や体制を整備することはセキュリティ対策の体制（どの委員会で決定するか）や担当部署を明確にすることは，後々のセキュリティ対策をスムーズに進めるうえで重要であることから，策定状況に関係なく一定割合で重要とみている。

管理的要素から見た情報についての対策に関しては，策定済の平均値が11.9％，策定中の平均値が11.2％，未策定の平均値が16.5％となっている。中央値との差もほとんど見られない。情報についての対策は，実施の難しさから，組織や体制の整備，情報システムの対策等に比して後回しにされることが多い。セキュリティポリシーの策定と運用において，情報の取り扱いに関する対策は，これまでの組織内での情報の取り扱いに関する考え方の変更や，取扱制限の実施で制限を設けることによる不自由さ等，他の対策項目よりも適切な運用を軌道に乗せるまでが難しい。セキュリティポリシー策定済の大学で，情報に関する対策の重要度が未策定の大学よりも低くなったのは，情報の取り扱いに関する学内での議論が完了し，規則の策定の目途がついたことで，検討項目の優先度が低くなったことが要因として考えられる。

管理的要素から見た情報処理についての対策に関しては，策定済の平均値が9.2％，策定中の平均値が10.3％，未策定の平均値が12.1％と大きな差は見られない。

管理的要素から見た情報システムについては，策定済の平均値が13.7％，策定中の平均値が15.2％，未策定の平均値が14.6％と策定中の平均値が高い点を除き大きな差は見られない。逆に中央値は，策定済と策定中が12.5％，未策定が14.5％と重要度が逆転しており，

策定中では平均値と中央値の差が目立つ。策定中の平均値が高くなったのは，セキュリティポリシーを策定中の大学での当面の検討項目にこの情報システムの対策が多く，重要と判断した回答があったため上に振れたことが考えられる。一般的にセキュリティポリシーは，まず組織や体制の整備，次に情報システムの対策，そして情報の対策，の順番で検討することが多い。策定中の多くの大学で，組織や体制の整備と情報システムの対策が検討されていて，情報の対策は必要性と重要性は認識しているが未着手，という状況であったことがうかがえる。

技術的要素から見た情報セキュリティに関する対策に関しては，策定済の平均値が25.4%，策定中の平均値が24.7%，未策定の平均値が22.6%と策定が進むにつれて重要度が高く評価されている。中央値は策定済と策定中が25%，未策定の中央値が24.0%となっており，未策定で平均値と中央値の差が目立つ。未策定の大学でこれらの項目の重要度をあまり評価しなかった回答があったことが平均値を下に振れされた要因と考えられる。

技術的要素から見た情報システムの構成要素に関しては，策定済の平均値が22.5%，策定中の平均値が19.5%，未策定の平均値が17.5%と策定が進むにつれて重要度が高く評価されている。中央値も策定済が20.0%，策定中が19.5%，未策定が16%と同様の傾向を示している。

3.3. 第3階層から見た第4階層

組織・体制の整備を行う項目からみた，その下の10項目についてみていく。組織・体制の整備の項目の中では，責任者や委員会を設置し組織・体制を定めることは策定済の平均値3.0%で中央値が2.8%，未策定の平均値が3.1%で中央値が3.3%と明確な差は見られないが，策定中の平均値は3.4%で中央値が2.5%と中央値だけ平均値が高く，中央値が低くなっている。策定中の標準偏差は3.4%と策定済の1.6%，未策定の1.8%と比しても大きく，策定中の大学でこれらの項目が具体的に検討されていることで重要視する回答者とそれほど重要視しない回答者が出ることで，ばらつきが大きくなったといえる。兼務が禁止される役割の規定，障害・事故への事前対応，自己点検，委託先への要求事項，についても同様に策定中であることで策定済，未策定より平均値が高くなり回答の分布が広くなっている。逆に違反への対処や例外措置，情報セキュリティ対策は策定中のみが重要度が低くなっている。ただ，違反への対処や例外措置は策定中のみが平均値も中央値も低いが，情報セキュリティ対策の中央値は策定済が2.3%，策定中が1.9%，未策定が1.7%と策定状況が進むにつれて重要度は上がっている。標準偏差も策定済が1.1%，策定中が1.8%，未策定が2.0%となっていることから，未策定の回答の中に重要視する回答が含まれて値が上に振

れたことが考えられる。

情報についての対策項目から見た，その下の６項目についてみていく。

情報の作成と入手，情報の利用，情報の保存，情報の移送，情報の提供，情報の消去であるが，すべての項目で重要度は，策定中，策定済，未策定の順で大きくなっている。標準偏差も未策定の情報の策定と入手，情報の利用，情報の移送，情報の消去で1.5％前後となった以外は1.0％前後とばらつきも小さく，ほぼ均一の回答であった。

情報処理についての対策に関する項目から見た，３項目についてみていく。情報システムの利用についての遵守事項を定めること，持込機器による情報処理の制限についての遵守事項を定めること，の２項目の重要度は策定済，策定中，未策定の順で平均値，中央値ともに大きくなっている。学外での情報処理の制限についての遵守事項を定めること，は他の２つと異なり，策定済のみ重要度が高くなっており，未策定では平均値と中央値の差も他よりも大きい。

大学では，教員や学生の私物パソコンやタブレット，スマートフォン等の情報機器の学内ネットワークへの接続が行われ，大学所管の備品以外のこれらの機器で成績処理をはじめとする情報処理が行われることがある。また，学外で出張時に携帯し出先で処理をすることもあり，規定を定め何かしらの制限を設ける必要があるが，これまで特段の制限がなかった行為に制限をかけると，制限をかけてセキュリティを維持することが目的であるにもかかわらず，制限されることを避けるために届け出をせずに機器を持ち出したり，許可されていない情報システムの利用方法を行ったりという事態が起きうるため，大学教職員のセキュリティレベルや意識を適切に把握し，制限のレベルを設定する必要があるが，設定は容易ではないためこのような結果になったのであろう。

情報システムについての基本的な対策を行うことから見た９項目についてみていく。情報システムのライフサイクル，機器等の購入について，ソフトウェア開発，不正プログラム感染防止について，ドメイン名の使用について，の５項目は，策定中が策定済と未策定より重要であると考えられている。学内でセキュリティポリシーの策定にあたりこれらの項目を検討したことで意識が高くなった回答があったことによると考えられる。主体認証・アクセス制御，権限管理等について，暗号と電子署名について，の２項目は３つの策定状況で平均値も中央値も同じような重要度となっている。この２項目はポリシーの策定状況に関わらず，情報システムの運用を行う上では重要な項目と，関係の有無がはっきりする項目であることから，策定状況が影響していない。情報システムに係る文書及び台帳整備，は策定が進んでいないほど重要度が高くなっている。策定済の大学では規則制定に伴い文書及び台帳の整備や棚卸が実施されたことで，重要度が相対的に低くなり，検討中の大学

では検討の途中で整備や棚卸を実施することでやや重要度が低くなったものと考えられる。学外の情報セキュリティ水準の低下を招く行為の防止について，は策定中のみが重要度が低くなっている。他の項目との相対的な配分で低くなってしまったのだと推測される。

情報セキュリティに関する要件から見たその下の 9 項目についてみていく。

主体認証に関する要件，証跡管理に関する要件，の 2 項目は，策定中が策定済，未策定に比して高く評価されている。セキュリティの機能として基本的なものであり，認証と証跡管理は個人の権利や権限に関わる項目であることから，厳密かつ適切な定義や運用が求められることから策定段階の担当者はこれらの項目への意識が高くなることは当然である。

セキュリティホール対策に関する要件，不正プログラム対策に関する要件，サービス不能攻撃対策に関する要件，踏み台対策に関する要件は未策定が策定済，策定中に比して重要度が低い。情報セキュリティに関する要件の重要度が策定済，策定中に比して低いことからこれらの項目も低くなっている。主体認証や証跡管理と異なり，セキュリティポリシーの策定の過程で初めて認識することも多い項目であることから，未策定の回答では重要視されていない。

権限管理に関する要件，暗号と電子署名に関する要件，は策定状況に関わらず重要度はほぼ同じ値であった。アクセス制御に関する要件，は策定中が策定済，未策定に比して低く評価されているが，中央値はほぼ同じ値であった。

情報システムの構成要素に関する要件から見た，その下の10項目についてみていく。情報システムを設置する安全区域，電子計算機共通の設置時・運用時及び運用終了時に関わる要件，サーバ装置の設置時・運用時及び運用終了時に関わる要件，DNS の導入時・運用時及び運用終了時に関わる要件，通信回線共通の対応，の 5 項目は策定状況が進むにつれて重要度が高くなっている。これらの項目は策定が進み運用されるにしたがって，策定した条文次第では運用・管理がままならないこともあり，表現内容に対してより慎重になっていくためである。端末の設置時・運用時及び運用終了時に関わる要件，学内回線の管理，の 2 項目は策定中のみが策定済，未策定よりも重要度が高くなっている。逆に電子メールの導入時・運用時及び運用終了時に関わる要件，は策定中のみが策定済，未策定よりも重要度が低くなっている。策定中のみが高くなるのは策定の検討途中に議論されたことによるものと考えることができ，低くなったのは，中央値で見ると策定中も未策定も同じ値であることから，相対的に重要度が低下したことによると考えられる。ウェブサーバの導入時・運用時及び運用終了時に関わる要件，学外回線の接続，の 2 項目は策定状況に関わらず重要度はほぼ同じである。

4. 策定状況による重要度の違い

ここからはいくつかの対策項目で，所属大学のセキュリティポリシーの策定状況による重要度の平均値の違いが有意な差であるかどうかを検証していく。なお，すべての仮説検定において，帰無仮説は策定済と未策定の母平均は等しい，対立仮説は管理に関する項目では策定済の母平均は未策定の母平均よりも重要度が小さいとし，技術に関する項目では策定済の母平均は未策定の母平均よりも重要度が大きいとしている。また，策定済と未策定のグループの分散は異なると仮定して検定している。

第３階層で有意な差がみられたのは４項目である。情報についての対策と情報処理についての対策は有意水準１％で，策定済と未策定の母平均は等しいという仮説は棄却され，策定済の母平均は未策定の母平均よりも重要度が小さいといえる。情報セキュリティに関する要件と情報システムの構成要素に関する要件は有意水準５％で，策定済と未策定の母平均は等しいという仮説は棄却され，策定済の母平均は未策定の母平均よりも重要度が大きいといえる。

表13　仮説検定の結果第３階層

情報についての対策

	策定済	未策定
平均	0.118846	0.165
分散	0.002806	0.005336
観測数	39	22
仮説平均との差異	0	
自由度	34	
t	-2.60263	
$P(T \leqq t)$ 片側	0.006804	
t 境界値 片側	1.690924	

情報処理についての対策

	策定済	未策定
平均	0.091538	0.121136
分散	0.001544	0.001919
観測数	39	22
仮説平均との差異	0	
自由度	40	
t	-2.62844	
$P(T \leqq t)$ 片側	0.006055	
t 境界値 片側	1.683851	

情報セキュリティに関する要件

	策定済	未策定
平均	0.253718	0.225455
分散	0.004547	0.003245
観測数	39	22
仮説平均との差異	0	
自由度	50	
t	1.739194	

情報システムの構成要素に関する要件

	策定済	未策定
平均	0.224487	0.174545
分散	0.010485	0.005721
観測数	39	22
仮説平均との差異	0	
自由度	55	
t	2.171569	

$P(T \leqq t)$ 片側	0.044077	$P(T \leqq t)$ 片側	0.017109
t 境界値 片側	1.675905	t 境界値 片側	1.673034

第 4 階層の管理面で有意な差がみられたのは，9 項目である。

情報についての対策項目の中の情報の作成と入手，情報の利用，情報の保存，情報の消去，情報処理についての対策の中の情報システムの利用については有意水準 1 %で，情報についての対策項目の中の情報の提供は有意水準 5 %で，組織・体制の整備の項目の中の見直しは有意水準10%で，策定済と未策定の母平均は等しいという仮説は棄却され，策定済の母平均は未策定の母平均よりも重要度が小さいといえる。

表14　仮説検定の結果管理面第 4 階層

情報の作成と入手

	策定済	未策定
平均	0.020596	0.031341
分散	0.000127	0.000289
観測数	39	22
仮説平均との差異	0	
自由度	32	
t	-2.65467	
$P(T \leqq t)$ 片側	0.006133	
t 境界値 片側	1.693889	

情報の利用

	策定済	未策定
平均	0.021513	0.030643
分散	0.000112	0.000215
観測数	39	22
仮説平均との差異	0	
自由度	34	
t	-2.57002	
$P(T \leqq t)$ 片側	0.007362	
t 境界値 片側	1.690924	

情報の保存

	策定済	未策定
平均	0.020115	0.026745
分散	0.000108	0.000101
観測数	39	22
仮説平均との差異	0	
自由度	45	
t	-2.44085	
$P(T \leqq t)$ 片側	0.009326	
t 境界値 片側	1.679427	

情報の消去

	策定済	未策定
平均	0.017724	0.02892
分散	0.000117	0.000226
観測数	39	22
仮説平均との差異	0	
自由度	34	
t	-3.07287	
$P(T \leqq t)$ 片側	0.002079	
t 境界値 片側	1.690924	

情報システムの利用

	策定済	未策定
平均	0.039551	0.062023
分散	0.000339	0.000801

情報の提供

	策定済	未策定
平均	0.020013	0.026202
分散	0.00011	0.000147

観測数	39	22
仮説平均との差異	0	
自由度	31	
t	-3.34656	
$P(T\leqq t)$ 片側	0.001078	
t 境界値 片側	1.695519	

観測数	39	22
仮説平均との差異	0	
自由度	39	
t	-2.00667	
$P(T\leqq t)$ 片側	0.025876	
t 境界値 片側	1.684875	

見直し

	策定済	未策定
平均	0.016141	0.010739
分散	0.000243	9.4E-05
観測数	39	22
仮説平均との差異	0	
自由度	58	
t	1.666676	
$P(T\leqq t)$ 片側	0.050485	
t 境界値 片側	1.671553	

第４階層の技術面で有意な差がみられたのは，６項目である。

情報セキュリティに関する要件のセキュリティホール対策，情報システムの構成要素の電子計算機共通の設置，DNS，通信回線，については有意水準５％で，情報セキュリティに関する要件のサービス不能攻撃対策，情報システムの構成要素の情報システムを設置する場所，については有意水準10％で，策定済と未策定の母平均は等しいという仮説は棄却され，策定済の母平均は未策定の母平均よりも重要度が大きいといえる。

表15　仮説検定の結果技術面第４階層

セキュリティホール対策

	策定済	未策定
平均	0.030749	0.023159
分散	0.000363	0.000218
観測数	39	22
仮説平均との差異	0	
自由度	53	
t	1.730416	
$P(T\leqq t)$ 片側	0.044688	
t 境界値 片側	1.674116	

電子計算機

	策定済	未策定
平均	0.019526	0.010705
分散	0.000544	0.00012
観測数	39	22
仮説平均との差異	0	
自由度	58	
t	2.001295	
$P(T\leqq t)$ 片側	0.025023	
t 境界値 片側	1.671553	

DNS

	策定済	未策定
平均	0.02191	0.013568
分散	0.000306	0.000259
観測数	39	22
仮説平均との差異	0	
自由度	47	
t	1.883448	
$P(T \leqq t)$ 片側	0.032918	
t 境界値 片側	1.677927	

通信回線

	策定済	未策定
平均	0.020167	0.011727
分散	0.000267	0.000134
観測数	39	22
仮説平均との差異	0	
自由度	56	
t	2.346823	
$P(T \leqq t)$ 片側	0.011248	
t 境界値 片側	1.672522	

サービス不能攻撃

	策定済	未策定
平均	0.021518	0.015659
分散	0.000304	0.000195
観測数	39	22
仮説平均との差異	0	
自由度	52	
t	1.434396	
$P(T \leqq t)$ 片側	0.078723	
t 境界値 片側	1.674689	

情報システムを設置する場所

	策定済	未策定
平均	0.023423	0.016545
分散	0.000273	0.000232
観測数	39	22
仮説平均との差異	0	
自由度	47	
t	1.64323	
$P(T \leqq t)$ 片側	0.053505	
t 境界値 片側	1.677927	

セキュリティポリシーが策定済の大学の担当者は，技術面の項目を重要視しており，未策定の大学の担当者は管理面の項目，特に情報についての対策を重視していることが明らかになった。

未策定の大学で情報についての対策が重要視された背景はアンケートの実施時期が2011年12月と東日本大震災から半年以上経過し事業継続や情報の可用性の確保についての議論が始まった時期であることから，それまで機密性，可用性，完全性のうち，機密性を重要視していた情報セキュリティ対策の考え方が情報の可用性も重要視されるようになり，未策定の大学の担当者としては，検討の対象や 3 要素のバランスについて検討が必要な環境となり，技術面での対応用より重視した意向が結果に表れているといえる。

策定済の大学においては，情報の取り扱いについてはセキュリティポリシー策定の過程で検討されたことで取り扱いについての要件を定めることについての合意が得られたことで相対的な重要度が低下し，逆に技術的な対応項目の実施に当たって組織内で直面している項目の重要度が高まっている。2011年には，フィッシング詐欺や不正アクセス，DDoS

攻撃，標的型攻撃，Web サイトからの情報流出等のセキュリティインシデントが世間を騒がせたため，これらに関連する技術的な項目が，策定済のポリシーで十分かさらなる改定や下位の規則での実対応の検討が意識されたことによると考えられる。

5. ま と め

私立大学のセキュリティ対策は，国立大学法人と比しても十分に行われているとは言えず，学内でのセキュリティ対策への意識の差も大きく十分な予算や人員の配置もままならない大学では担当者の負担が大きい。セキュリティ対策を進めるために必要な，人材，予算，権限のうち，本論文では人材中でも組織内での推進役になるセキュリティ担当者の意識が，所属する私立大学のセキュリティポリシーの策定状況の違い，言い換えれば，セキュリティポリシーの策定過程での組織や体制，情報の取り扱い，情報処理の体制，情報システムの管理，情報セキュリティの要件，情報システムの構成要素の対策というセキュリティ対策を検討し学内で議論を重ねてセキュリティ関連規則として体系づけを行っているかどうかで対策項目の重要度の配分が異なることがアンケート調査の分析で明らかになった。セキュリティ対策の PCDA サイクルを回し，セキュリティレベルを上げていくためにも学内での議論は必要で，議論を通して重きを置く項目が管理面，特に情報の取り扱いから技術的な対応項目へとシフトし，なるべく項目を均一に重要視するように変化していくことが明らかになった。

今後もクラウドサービスを始めとする新しい技術の登場やセキュリティの脅威，社会の意識等変化し続ける環境下でのセキュリティ担当者の意識の推移を調査し，組織内でセキュリティ対策を推進する要因，阻害する要因についての研究を発展させる必要があろう。

参 考 文 献

［1］ 私立大学情報教育協会，“私立大学情報環境白書（平成23年度版），”2012年.
［2］ 私立大学情報教育協会，“私立大学情報環境白書（平成20年度版），”2009年.
［3］ 木下栄蔵，“AHP とコンジョイント分析，”木下栄蔵・大野栄治編，現代数学社，東京，2004.
［4］ 内閣官房情報セキュリティセンター，“政府機関の情報セキュリティ対策のための統一管理基準解説編，”2011年.
［5］ 内閣官房情報セキュリティセンター，“政府機関の情報セキュリティ対策のための統一技術基準解説編，”2011年.
［6］ 小川賢，辻正次，“地域 EHR の推進要因，”日本遠隔医療学会雑誌，Vol. 8, No. 2，pp. 242-245. 日本遠隔医療学会，2012年９月.
［7］ 小川賢，“私立大学情報セキュリティ担当者への情報セキュリティ対策に関するアンケー

ト調査について，”電子情報通信学会技術報告，電子情報通信学会，vol. 112, No. 26, pp. 13-18. 2012年 5 月.
［8］ 曽根秀昭他，“高等教育機関の情報セキュリティ対策のためのサンプル規程集，”曽根秀昭（編），国立情報学研究所ネットワーク運営・連携本部国立大学法人等における情報セキュリティポリシー策定作業部会電子情報通信学会ネットワーク運用ガイドライン検討ワーキンググループ，2007.
［9］ 刀根薫，“ゲーム感覚意思決定法，”日科技連出版社，東京，1986.