私立大学情報セキュリティ担当者の CSIRT に関するアンケート調査

小　川　　賢

1. は　じ　め　に

日本に600校余りの私立大学があり，学校基本調査によると，学生数で約213万人，雇用されている教員数で10.7万人，職員数14.4万人の規模に上り[1)]，国立大学の86校，学生数61万人，教員数6.4万人，職員数８万人，公立大学の90校，学生数15万人，教員数1.3万人，職員数1.6万人と比しても高等教育機関の中では大きい存在である。

大学というカテゴリーでは国公立大学も私立大学も同じで，入試に関するミスや様々なインシデントが世間に与える影響は，設置の形態は関係ない。また，学生の成績や生活状況を含む個人情報，研究成果に関する情報，教職員の個人情報等，扱う情報の種類もほぼ同様で，情報を盗もうと意図する者からすれば同じといえる。

しかしながら，国立大学法人と異なり，文部科学省からの事務連絡によるセキュリティ対策の実施や中期行動計画へのセキュリティ対策の反映などが求められておらず，教職員の間には相当の差が存在している。ここ数年は，文部科学省から私立大学へのセキュリティ対策の事務連絡も送られており，私立大学もセキュリティ対策の推進が求められている。しかしながら，情報化推進室による詳細な連絡がある国立大学法人と異なり，十分な情報提供がなされているとはいえない（小川［2015］）。

この差は，情報セキュリティ対策に関するコミュニティの有無とも関連しているともいえる。巧妙化された攻撃を，自組織だけでのセキュリティ対策には限界があり，組織外とインシデント情報や攻撃の手口等セキュリティに関する動向や情報を共有し，自組織の対策に反映させることで，自組織のセキュリティ対策のレベルを上げることが必要となっている。外部のセキュリティベンダーを活用していても常に未知のマルウェアによるネットワーク内での感染リスクがあり，外部リソースの活用が迅速な対応を取るためには必要条件となりつつある。

そのような中で大学においても，CSIRT を設置する動きが始まっており，国立大学法

人においては，多くの高等教育機関がセキュリティ対策に参考にしている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にもCSIRT設置に関する規則が収録されており[2)]，その動きは今後私立大学にも及ぶことは容易に想像できる（小川［2017］，［2018］）。

本稿では，アンケートを通じて，全国の私立大学の情報セキュリティ担当者がCSIRTの設置や学内の情報セキュリティ対策を取り巻く環境についてどのように考えているかを明らかにし，今後の私立大学における情報セキュリティ対策を推進していくための課題を明らかにする。

2．CSIRTの活動に関する先行研究

セキュリティ対策の推進に関する研究は多く存在するが，CSIRTの活動，特に活動の阻害要因についての研究としては，これらがあげられる。

見目他［2013a］，見目他［2013b］では，CSIRTの活動が進んでいない要因としてCSIRTの高コスト構造に着目し，人的資源管理方式に焦点を当てて提案したトリアージ戦略と脆弱性評価システムの評価基準を合わせたアルゴリズムによる高コスト構造の削減と，LoA（Level of Assurance）の適用を図ることでレベル分けを行うことで低コスト化の提案と効果の可視化が行えることで経営者の判断を容易にすることができることを示している。

菊池，谷本［2011］では，CSIRTの普及を促すための活動とコストとの関係について考察し，対象とするプロジェクトを構造化，細分化することでその規模を見積もる手法であるWBS（Work Breakdown Structure）手法によってCSIRTのコスト構造の可視化を試みている。

3．アンケート調査

3.1　アンケートの概要

アンケートは2017年９月に全国602の私立大学の情報セキュリティ担当者に郵送し，131の回答があった。回収率21.8％であった。それぞれの質問に対して，全くそう思わない／あまりそう思わない／どちらともいえない／ややそう思う／強くそう思う，の５段階の記述で質問した。

3.2　アンケートの記述統計

ここからはアンケートの集計結果について述べていく。全くそう思わないを１，あまり

そう思わないを２，どちらともいえないを３，ややそう思うを４，強くそう思うを５とみなして，記述統計を見ていく。

CSIRTの設置については，回答のあった私立大学で設置されていると回答したのは10校で，121校は設置されていない，との回答であった。国立大学法人は文部科学省からの通知で設置が進んでいるが，アンケート対象とした私立大学では設置が進んでいない現状が明らかになった。設置されている10校にCSIRTが機能しているかについて尋ねたところ，どちらともいえないが４校，ややそう思うが３校，その他が１校ずつで，最頻値は３であったが，全体としては担当者の想定よりもやや機能していると考えているといえる。

設置されていない121校に，CSIRTが設置された場合機能すると思うか尋ねたところ，全くそう思わないが12，あまりそう思わないが28，どちらともいえないが49，ややそう思うが30，強くそう思うが２となり，最頻値は３であった。すでに設置している大学の担当者との比較ではやや機能することへの期待がみられるが，設置しても十分に機能するとは考えていないことがうかがえる。

大学の経営陣に対する評価についての項目は次のとおりである。

大学の経営陣のセキュリティインシデントへの対応についてどのように考えているかの質問はインシデント発生時の業務への影響を予測できると思うか，セキュリティリスクを管理する仕組みの構築・運用ができていると思うか，を尋ねた質問では，どちらも否定的な評価が多く，最頻値は２であった。セキュリティインシデントの経験がないと業務に与える影響の予測は容易ではないが，担当者が望むレベルで，経営陣がセキュリティインシデントを危機としてとらえていなかったり，予算や人員が割り当てられていなっかったりすることから経営陣のセキュリティインシデントに対する評価が低くなっているのであろう。

教職員が所属大学に誇りを持っていると考えているか，教職員が所属大学の社会的プレゼンスを理解していると思うかに対して，どちらも最頻値が４で，次いで３が多く，所属する教職員の大学に対する帰属意識についてはやや高いと考えている。近年の私立大学を取り巻く環境の厳しさや社会的プレゼンスが求められている現状がこのような結果をもたらしたのであろう。

最近のサイバーセキュリティ対策について，自組織だけで行うことへの限界については最頻値が５と，多くの回答者が自組織での対策には限界があると考えている。攻撃の巧妙化で侵入されていることも気づかないまま数か月経過する場合も散見されており，外部組織，外部機関の活用なしでセキュリティの維持が困難となってきていることを認識した結果であろう。

所属大学の教職員がセキュリティインシデントを起こすことを社会に対して恥ずかしいと考えているかについては最頻値が５と高く，大学がセキュリティインシデントで世間を騒がせてしまうことへの抵抗が強いことがうかがえる。教育機関の社会的プレゼンスを踏まえて考えると，不祥事で大学の名前が出てしまうことに対する抵抗の強さがみられる。

所属教職員のセキュリティポリシーの認識は最頻値が２とやや低く評価ししている。セキュリティポリシーの制定や運用が中期行動計画に記載されている国立大学法人と異なり，セキュリティ対策の実施について国立大学法人ほど求められていない私立大学においては当然の結果といえる。

インシデントの経験は危機管理に活きるか尋ねた質問では，最頻値が４で，次いで５と高く考えている。復旧可能な程度のインシデントの経験は危機管理では有効であると考えている。危機管理能力の高さについては，最頻値が３であるが，次に多いのは２で，やや低いと考えている。

インシデント発生時のダメージコントロール，IR 対応については，どちらも最頻値が３であるが，ダメージコントロールについては，３を中心のピークとした山型の分布をしているが，IR 対応については２も３とほぼ同数で，十分にコントロールができておらず，IR 対応も十分でないと考えていることがうかがえる。

CSIRT の活動と組織内の権限についての質問についての回答は次のようになっている。

CSIRT が機能するためには学内で自由に活動できることが必要かについては，最頻値が４と高く，４と５の回答で全体の69％を占めていた。一方で，CSIRT が機能するためにインシデント情報を外部に制約なしに提供できることが必要かについては，最頻値が３と学内での活動の自由度の高さに比して，低い回答であった。学外への情報提供については抵抗が強いことがうかがえる。

組織内でのコミュニケーションについては，部署を超えてのコミュニケーションも，同じ部署でのコミュニケーションの最頻値は３，上司と部下のコミュニケーションの最頻値は４であるが，部署を超えては３と４で71％，上司と部下では３と４で85％を占めていた。おおむね組織内の風通しはよいと考えていることがうかがえる。

CSIRT の効果についての質問は次のとおりである。

CSIRT が有効に機能するとインシデント対応の時間・コスト短縮につながると思うかに対しては，最頻値が４で４と回答した割合が45％であった。５を含めると４と５で70％が時間・コスト短縮の効果があると考えている。

CSIRT が有効に機能すると情報漏えいの防止・漏えいリスクの低下につながると思うかに対しては，最頻値が４で４と回答した割合が50％であった。５を含めると４と５で75

%が情報漏えいの防止・漏えいリスクの低下効果があると考えている。

CSIRTが有効に機能すると社会での大学の信頼の維持につながると思うかに対しては，最頻値が4で4と回答した割合が42%であったが，この項目のみ他3つと異なり3と4で全体の約75%が大学の信頼の維持につながると考えており，期待する効果がやや低くなっている。

CSIRTが有効に機能すると学内で発生する重大インシデントの減少につながると思うかに対しては，最頻値が4で4と回答した割合が46%であった。5を含めると4と5で70%が重大インシデントの低下につながると考えている。

CSIRTが有効に機能した場合の効果については高い期待を持っていることがアンケートの結果わかる。

所属大学のセキュリティインシデント対応が機能している/すると思うかに対しては，最頻値は3で3と回答した47.3%をピークとした対称的な分布になっている。

自身の所属大学のインシデント対応については可もなく不可もなく機能していると判断していることがうかがえ，CSIRTの効果についての設問と合わせて読み解くとCSIRTによる機能の強化に対する期待がみられる。

自身のセキュリティに対する感覚についての項目は次の通りである。

自分がセキュリティに対する意識が高いと思うかについては，最頻値は4で4と回答した割合が55%であった。3と4で80%を占めている。

セキュリティ対策の実施でインシデント発生の減少の関係については，最頻値が4で4と回答した割合が49.6%で4をピークに3と5にほぼ同数の回答が分布している。

セキュリティ対策の実施と志願者数の関係については，最頻値は3で，3と回答した割合が36.6%，3と4で約66%を占めている。セキュリティ対策の実施状況が志願者数に影響を及ぼすと考えられている組織であれば，志願者確保が私立大学の経営においては最重要項目であることから，組織内でセキュリティ対策の実施にも積極的になるが，現状では，相関は低いと考えられている。私立大学のセキュリティ対策の実施を促進する要因が現時点では，監督官庁である文部科学省からの事務連絡以外に見当たらない。

業務上でのヒヤリハットの経験については，最頻値が2で2と回答した割合が37.4%であった，2と3で68%を占めている。学外に公表しなければならないレベルではないにせよ，インシデントやインシデントになりかねない事案は定期的に発生しており，担当者としては日常的に緊張を強いられていることがうかがえる。

自身のコミュニケーション能力についての質問では，最頻値が3で，3と回答した割合が53.4%で3を中心とした対称的な分布をとっている。CSIRTは自組織内での対応だけで

なく，他組織とのコミュニケーションを通して自組織のセキュリティ能力を向上させていくことが重要となり，コミュニケーション能力の自負は他組織との情報共有において重要な要因となるため，担当者の意識を尋ねた。

すでに出来上がっているコミュニティへの参加についての質問では，最頻値が３で，３と回答した割合が48.1％で３を中心とした対称的な分布をとっている。CSIRT の普及はこれまで地道に活動してきた先導的な人たちの貢献によるところが大きく，先導的な人たちは意識していない場合でも，すでにコミュニティが出来上がり，そこに入っていくことが障壁に感じられてしまうこともありうるが，担当者は特段の障壁には感じていないようである。

アンケートの結果からは，CSIRT 設置の効果に対する期待は大きいが，CSIRT の設置は進んでおらず，セキュリティ対策全般に対する予算や人員等が十分に配分されていないことから，経営陣のセキュリティ対策への意識が低いと担当者が認識していることがみられる。学内の意識はそれなりにあるものの，セキュリティ対策の実施と社会的信用や志願者数への影響にはつながるとは考えておらず，組織内でセキュリティ対策をさらに進めていく決め手を欠いているという状況がみられる。

CSIRT の特徴は，組織の枠を超えたインシデント情報の共有にある。組織外での新たな脅威の情報を自組織での対策に反映させることが可能な一方，自組織のインシデント情報も外部に提供することになる。担当者レベルでは必要かつ有用と認識しても，経営陣が難色を示す場合もあり，どれだけ，経営陣がセキュリティ対策の必要性と，自組織での限界に理解を示すかが分水嶺となる。アンケートからは担当者レベルでは自組織の情報提供，自身のコミュニティへの参加に対する抵抗はあまり見受けられないが，経営陣，学内の同意が得られるかについては懐疑的な見方を持っているようである。

表１　アンケートの回答

以下の質問にお答えください。	1	2	3	4	5
１．所属組織には **CSIRT** が設置されていますか。	10	121			
２．設置されている **CSIRT** は機能していると思いますか。	1	1	4	3	1
３．設置されるとしたら **CSIRT** は機能すると思いますか。	12	28	50	30	2
４．経営者は現時点での脆弱性を把握し，インシデント発生時の業務への影響を予測できると思いますか。	34	61	24	8	4
５．経営者は，組織のサイバーリスクを認識し，主体的にセキュリティリスクを管理する仕組みを構築・運用できていると思いますか。	35	57	29	9	1
６．貴学の教職員は，貴学に誇りを持っていると思いますか。	2	9	46	59	15
７．貴学の教職員は，貴学の社会的プレゼンスを理解していると思いますか。	2	13	43	63	10

9．貴学の教職員が，セキュリティインシデントを起こしてしまうことは社会に対して恥ずかしいことだと思いますか。	1	5	19	37	69
10．貴学の教職員は，貴学のセキュリティポリシーを知っていると思いますか。	24	55	31	19	2
11．インシデントの経験は危機管理に活きると思いますか。	0	5	16	65	45
12．貴学の危機機管理能力は高いと思う。	16	36	57	20	2
13．貴学は，インシデント発生時に，迅速かつ適切な初動対応による被害拡大抑制（ダメージコントロール）をとることができると思いますか。	10	36	57	25	3
14．貴学は，インシデント発生時に，学生や保護者とのコミュニケーション，広報部門・法務部門と連携しながらの危機時の IR 対応（レピュテーションマネジメント）をとることができると思いますか。	14	44	45	26	2
15．CSIRT が組織内で有効に機能するためには，CSIRT が学内で制約なく自由に活動できることが必要であると思いますか。	2	12	26	48	43
16．CSIRT が組織内で有効に機能するためには，セキュリティ対策に関する学内の情報を，CSIRT の判断で外部機関に制約なく提供できることが必要であると思いますか。	5	30	45	37	14
17．貴学では部署を超えた教職員のコミュニケーションがとれていると思いますか。	4	27	45	49	6
18．貴学では同じ部署内の上司と部下のコミュニケーションがとれていると思いますか。	3	9	53	60	6
19．CSIRT が有効に機能するとインシデント対応の時間・コスト短縮になると思いますか。	2	11	26	59	33
20．CSIRT が有効に機能すると情報漏えいの防止・漏えいリスクの低下につながると思いますか。	3	8	23	65	32
21．CSIRT が有効に機能すると，社会での貴学の信頼が維持されると思いますか。	4	10	43	55	19
22．CSIRT が有効に機能すると，学内で発生する重大インシデントの減少につながると思いますか。	5	8	26	61	31
23．貴学のセキュリティインシデント対応は機能している／機能すると思いますか。	6	31	62	31	1
24．自分はセキュリティに関する意識が高いと思いますか。	2	11	33	72	13
25．セキュリティ対策を実施するとインシデントの発生は減少すると思いますか。	1	12	29	65	24
26．セキュリティ対策を実施してもしなくても志願者数には影響しないと思いますか。	7	22	48	39	15
27．業務上でセキュリティ関係のヒヤリハットの経験がありますか。	24	49	41	15	2
28．自分はコミュニケーション上手だと思う。	4	30	70	26	1
29．すでに出来上がっているコミュニティに参加するのは躊躇してしまう。	8	26	63	28	6
30．自分はサイバーセキュリティに対する意識が高いと思う。	2	14	45	62	8

4．回答者の意識による回答の比較

ここでは，アンケートの結果を回答者の意識で分類し，回答者の意識で回答に違いがみられるかを分析していく。

アンケートの回答者を次の３つの質問でウォード法を用いて３グループに分けた。

・セキュリティに関する意識が高いと思うか

・セキュリティ対策を実施するとインシデントの発生は減少すると思うか
・セキュリティ対策を実施しても志願者数には影響しないと思うか

クラスター１は回答者の意識も高くセキュリティ対策の効果も大学運営に与える影響も大きいと考えるグループ，クラスター２は意識もそれなりに高く対策の効果もあるが，大学運営に与える影響は軽微であると考えるグループ，クラスター３は，意識も高くなくセキュリティ対策の効果も大学運営に与える影響もそれほどではないと考えるグループ，とした。

4.1　質問項目別の違い

グループの違いによって，アンケートの回答に違いがみられるか，まずは各質問項目の単純集計から見ていく。

CSIRT が設置された場合機能すると思うか尋ねたところ，「クラスター１」は，３を中心とした対称分布であったが，「クラスター２」は３と４に集中しており，「クラスター３」は３が最大数で２がそれに次ぐ分布であった。

大学の経営陣のセキュリティインシデントへの対応についてどのように考えているかの質問は，インシデント発生時の業務への影響を予測できると思うか，セキュリティリスクを管理する仕組みの構築・運用ができていると思うか，を尋ねた質問では，どちらも否定的な評価が多かった。クラスター１と３は２と回答した割合が最も多く，次いで１であったが，クラスター２では１と２の回答が同じ割合と，他のクラスターに比して経営陣に対する評価が低かった。

教職員が所属大学に誇りを持っていると考えているか，教職員が所属大学の社会的プレゼンスを理解していると思うかに対しても，大学の経営陣のセキュリティインシデントへの対応についてどのように考えているかの質問と同様に，クラスター１と３は４と回答した割合が最も多く，次いで３であったが，クラスター２では３と４の回答が同じ割合と，他のクラスターに比して経営陣に対する評価が低かった。

最近のサイバーセキュリティ対策について，自組織だけで行うことへの限界についてはどのクラスターも５と回答した割合が最も多かったが，ここでもクラスター２だけ割合が低く，４と回答した割合も５に次いで多かった。

所属大学の教職員がセキュリティインシデントを起こすことを社会に対して恥ずかしいと考えているかについてはどのクラスターも５と回答した割合が最も多かったが，その突出の程度は，クラスター１，クラスター２，クラスター３の順で低くなっている。

所属教職員のセキュリティポリシーの認識はどのクラスターでも最頻値は２であったが，

分布をみると，クラスター１と３は最頻値が２でついで３の回答が多い同じような分布であったが，クラスター２のみ１の回答も多く低く評価ししていることがわかる。

インシデントの経験は危機管理に活きるか尋ねた質問では，クラスター１のみ最頻値が５と高くなっているが，クラスター２と３では最頻値は４とやや低い。さらに，その回答割合をみると，クラスター３は４に集中しているが，クラスター２は４に次いで５という分布と違いが出ている。

自組織の危機管理能力の高さについての評価は，どのクラスターも３の回答が最も多かったが，クラスター１は３を中心とした対称的な分布であったが，クラスター２と３では２番目に高かった２の割合が多く，違いがみられた。

インシデント発生時のダメージコントロール，については，どのクラスターも３が最頻値であったが，クラスター２は３を中心とした対称的な分布であったが，クラスター１は２番目に高かった４の割合が多く，クラスター３は２番目に高かった２の割合が多くここでも違いがみられた。

IR 対応については，クラスター１は最頻値が２で，３と４が２とほぼ同じ割合の回答であった。クラスター２と３はどちらも最頻値が３であるが，ほぼ同じ割合の回答で２が２番目に多かった。

CSIRT が機能するためには学内で自由に活動できることが必要かについては，クラスター１と２では最頻値が５，次いで４と高い評価であったが，クラスター３は最頻値が４で，ほぼ同数で３，次いで５とクラスター１と２に比して低く評価されている。

CSIRT による外部への情報提供については，クラスター１と３では最頻値が３，次いで４と高い評価であったが，クラスター２では，最頻値は２，ついで４と２つのピークをもつ分布となっており，CSIRT による学部への情報提供については意見が分かれている。

組織内でのコミュニケーションについては，部署を超えてのコミュニケーションについては，CSIRT による外部への情報提供と同様の傾向がみられ，クラスター１と３では最頻値が３，次いで４と高い評価であったが，クラスター２では，最頻値は２，ついで４と２つのピークをもつ分布となっている。

同じ部署でのコミュニケーションについては，クラスター１と２では最頻値が４でついで３と２つに回答が集中しているが，クラスター３は最頻値が３でついで４と３と４に回答が集中している。３と４に集中する点はどのクラスターにも共通しているが，評価値は若干の差がみられた。

CSIRT が有効に機能するとインシデント対応の時間・コスト短縮につながると思うかに対しては，どのクラスターも最頻値が４であったが，クラスター１と２では２番目に多

かった回答は５であったが，クラスター３では２番目に多かったのは３であった。クラスター１と２の回答の分布をみると，クラスター１では４と５はほぼ同数であったが，クラスター２では，２番目に多かった５は最頻値の４の66.7％の割合で，傾向に差がみられた。CSIRT が有効に機能すると情報漏えいの防止・漏えいリスクの低下につながると思うかに対しても同様の傾向がみられた。

CSIRT が有効に機能すると社会での大学の信頼の維持につながると思うかに対しては，クラスター１と２で最頻値が４であったが，クラスター１は４を中心として，３と５がほぼ同数の分布，クラスター２は４に次いで３のみが多い分布，クラスター３では最頻値の３に次いで４が多い分布となった。クラスター２と３は分布の傾向が近いといえる。クラスター１は社会での信頼や評価が，クラスター２と３よりも意識されていることがわかる。

CSIRT が有効に機能すると学内で発生する重大インシデントの減少につながると思うかに対しては，どのクラスターも最頻値は４であったが，２番目に多い回答が，クラスター１と２では５，クラスター３では３と違いがみられた。

表２　クラスター別回答状況

	クラスター１					クラスター２					クラスター３				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
１．**CSIRT** が設置されていますか。	6	36	0	0	0	2	36	0	0	0	2	49	0	0	0
２．設置されている **CSIRT** は機能していると思いますか。	1	1	2	1	0	0	0	1	2	0	0	0	1	0	1
３．設置されるとしたら **CSIRT** は機能すると思いますか。	1	10	15	10	1	4	5	13	13	1	7	13	22	7	0
４．経営者は現時点での脆弱性を把握し，インシデント発生時の業務への影響を予測できると思いますか。	8	21	6	3	4	14	14	8	2	0	12	26	10	3	0
５．経営者は，組織のサイバーリスクを認識し，主体的にセキュリティリスクを管理する仕組みを構築・運用できていると思いますか。	10	15	13	3	1	13	13	10	2	0	12	29	6	4	0
６．貴学の教職員は，貴学に誇りを持っていると思いますか。	0	1	13	20	8	1	3	14	15	5	1	5	19	24	2
７．貴学の教職員は，貴学の社会的プレゼンスを理解していると思いますか。	0	2	14	20	6	1	1	14	19	3	1	10	15	24	1
８．昨今のサイバーセキュリティ対策を，自組織だけで行うことは限界があると思いますか。	0	1	1	12	28	0	2	5	13	18	0	2	3	14	32
９．貴学の教職員が，セキュリティインシデントを起こしてしまうことは社会に対して恥ずかしいことだと思いますか。	1	0	3	10	28	0	2	3	11	22	0	3	13	16	19
10．貴学の教職員は，貴学のセキュリティポリシーを知っていると思いますか。	5	19	11	6	1	10	13	7	7	1	9	23	13	6	0

11. インシデントの経験は危機管理に活きると思いますか。	0	1	3	15	23	0	2	4	18	14	0	2	9	32	8
12. 貴学の危機機管理能力は高いと思う。	4	9	18	9	2	6	11	14	7	0	6	16	25	4	0
13. 貴学は，インシデント発生時に，迅速かつ適切な初動対応による被害拡大抑制（ダメージコントロール）をとることができると思いますか。	2	8	19	12	1	3	9	16	9	1	5	19	22	4	1
14. 貴学は，インシデント発生時に，学生や保護者とのコミュニケーション，広報部門・法務部門と連携しながらの危機時の IR 対応（レピュテーションマネジメント）をとることができると思いますか。	4	14	11	12	1	3	12	13	9	1	7	18	21	5	0
15. CSIRT が組織内で有効に機能するためには，CSIRT が学内で制約なく自由に活動できることが必要であると思いますか。	0	3	7	16	16	1	5	2	14	16	1	4	17	18	11
16. CSIRT が組織内で有効に機能するためには，セキュリティ対策に関する学内の情報を，CSIRT の判断で外部機関に制約なく提供できることが必要であると思いますか。	2	6	16	12	6	1	12	9	10	6	2	12	20	15	2
17. 貴学では部署を超えた教職員のコミュニケーションがとれていると思いますか。	2	5	17	17	1	0	11	9	13	5	2	11	19	19	0
18. 貴学では同じ部署内の上司と部下のコミュニケーションがとれていると思いますか。	0	1	17	23	1	1	2	14	17	4	2	6	22	20	1
19. CSIRT が有効に機能するとインシデント対応の時間・コスト短縮になると思いますか。	0	2	6	18	16	0	4	4	18	12	2	5	16	23	5
20. CSIRT が有効に機能すると情報漏えいの防止・漏えいリスクの低下につながると思いますか。	0	2	4	20	16	1	0	6	19	12	2	6	13	26	4
21. CSIRT が有効に機能すると，社会での貴学の信頼が維持されると思いますか。	0	1	9	22	10	2	4	12	15	5	2	5	22	18	4
22. CSIRT が有効に機能すると，学内で発生する重大インシデントの減少につながると思いますか。	0	1	7	20	14	1	3	5	18	11	4	4	14	23	6
23. 貴学のセキュリティインシデント対応は機能している／機能すると思いますか。	1	11	16	13	1	2	7	17	12	0	3	13	29	6	0
24. 自分はセキュリティに関する意識が高いと思いますか。	0	0	1	31	10	0	2	8	25	3	2	9	24	16	0
25. セキュリティ対策を実施するとインシデントの発生は減少すると思いますか。	0	0	3	26	13	0	0	1	26	11	1	12	25	13	0
26. セキュリティ対策を実施してもしなくても志願者数には影響しないと思いますか。	6	13	23	0	0	0	0	0	28	10	1	9	25	11	5
27. 業務上でセキュリティ関係のヒヤリハットの経験がありますか。	5	15	15	5	2	9	18	8	3	0	10	16	18	7	0
28. 自分はコミュニケーション上手だと思う。	1	6	24	11	0	0	12	17	8	1	3	12	29	7	0
29. すでに出来上がっているコミュニティに参加するのは躊躇してしまう。	3	9	19	9	2	3	10	14	11	0	2	7	30	8	4

30. 自分はサイバーセキュリティに対する意識が高いと思う。	0	0	9	28	5	0	3	11	21	3	2	11	25	13	0

4.2　分散分析

次に，それぞれの質問項目についてクラスターによる違いを分散分析でみていく。分散分析の結果は表３から表７のようになり，次の６項目でクラスター間での有意な差がみられた。

・インデント発生時のダメージコントロールについて（有意水準５％）
・部署内の上司と部下とのコミュニケーションについて（有意水準10％）
・CSIRT によるインシデント対応の時間・コスト短縮について（有意水準１％）
・CSIRT による情報漏えいの防止，漏えいリスクの低下について（有意水準１％）
・CSIRT による大学の社会での信頼の維持について（有意水準１％）

所属大学のインシデント発生時のダメージコントロールをとることができると思うかについては，クラスター１は３と４に，クラスター２は３にクラスター３は３と２に回答が集中した。セキュリティに対する意識が高いクラスターほど，コントロールできると考えており，セキュリティの意識の高さとクダメージコントロールの関係の高さがみられる。

部署内の上司と部下のコミュニケーションについては，クラスター１では４と３，クラスター２も同じく４と３であるが，クラスター１は４の割合が多いがクラスター２は４と３の回答数の差はクラスター１より少なく１よりも低い評価となっている。さらにクラスター３は３と４とクラスター２より，低い評価となっている。

CSIRT によるインシデント対応の時間・コスト短縮については，クラスター１と２では４が最多でついで５，クラスター３では４が最多でついで３となっている。クラスター１はクラスター２と比して５や３と回答した数が多い。CSIRT の活動による効果に対しては，クラスター１のセキュリティ意識が高くセキュリティ対策によるインシデント低減の効果を考えている回答者ほど，CSIRT によるインシデント対応の時間・コスト短縮を考えていることが明らかになった。CSIRT による情報漏えいの防止，漏えいリスクの低下についても，CSIRT によるインシデント対応の時間・コスト短縮についてと同様の傾向がみられる。

CSIRT による大学の社会的信頼の維持については，クラスター１は４の回答が最多でついで５，ほぼ同数で３と高い評価となっている。クラスター２は４の回答が最多でついで３，クラスター３は３の回答が最多でついで４となっている。

クラスターで有意な差がみられたこれらの項目と，回答の傾向を考察していく。セキュ

表３　分散分析　インデント発生時のダメージコントロール

変動要因	変動	自由度	分散	観測された分散比	P-値	F 境界値
グループ間	6.117847	2	3.058924	3.834471	0.024137	3.066952
グループ内	102.1112	128	0.797743			
合計	108.229	130				

表４　分散分析　部署内の上司と部下とのコミュニケーション

変動要因	変動	自由度	分散	観測された分散比	P-値	F 境界値
グループ間	3.341552	2	1.670776	2.782564	0.065627	3.066952
グループ内	76.85692	128	0.600445			
合計	80.19847	130				

表５　分散分析　CSIRT によるインシデント対応の時間・コスト短縮

変動要因	変動	自由度	分散	観測された分散比	P-値	F 境界値
グループ間	11.78485	2	5.892424	7.125548	0.001164	3.066952
グループ内	105.8487	128	0.826943			
合計	117.6336	130				

表６　分散分析　CSIRT による情報漏えいの防止，漏えいリスクの低下

変動要因	変動	自由度	分散	観測された分散比	P-値	F 境界値
グループ間	14.10057	2	7.050285	9.213685	0.000183	3.066952
グループ内	97.94523	128	0.765197			
合計	112.0458	130				

表７　分散分析　CSIRT による大学の社会での信頼の維持

変動要因	変動	自由度	分散	観測された分散比	P-値	F 境界値
グループ間	10.35681	2	5.178404	6.391596	0.00226	3.066952
グループ内	103.7043	128	0.81019			
合計	114.0611	130				

リティ意識が高くセキュリティ対策によるインシデント低減の効果を考えているクラスターほど，インシデント発生時のダメージコントロールが可能であると考えている。また，組織の風通しがいいと考えている。さらに，CSIRT によるインシデント対応の時間・コス

トの短縮，情報漏えいの防止，漏えいリスクの低下，大学の社会での信頼の維持がなされることへ評価が高くなっている。

5．結　　論

私立大学のセキュリティ担当者に対するアンケート調査を単純集計と回答者の意識によるクラスターの比較を通して，CSIRT への期待と，自組織のセキュリティ対策の状況，経営陣の意識，予算と人員，教職員のセキュリティに対する意識，組織の硬直性等の関係を考察した。

担当者が，自身のセキュリティ意識が高く，自組織でセキュリティ対策を実施すると効果が高いと考えているほど，CSIRT 導入による効果に対する期待が高いことが明らかになった。CSIRT の活動はネットワーク外部効果を活用したものと考えることができ，外部のリソースを活用することに意義がある。その為，すでに構築され活動しているコミュニティへの参加に対する積極性が求められるが，アンケートに協力いただいた回答者は，組織の了解が取れれば積極的に参加して自組織のセキュリティレベルの維持向上に貢献する意欲は見られる。あとは，いかに組織として意欲のある担当者を支援して，自組織のセキュリティ対策を維持し続けるかによるところが大きいといえる。

現在のところ，高等教育機関，特に私立大学に対するセキュリティ対策は，すべての私立大学を包括する取り組みはなされておらず，私立大学情報教育協会をはじめとする，一部組織による活動だけである。担当者レベルでは，国立大学法人の担当者との情報共有もなされているが，組織としての協働はなかなか進んでおらず，協働を開始することが私立大学を取り巻く課題である。大学の経営陣がインシデントに関するリスクについて情報共有することがセキュリティレベルの低下とコストの増加を防ぎ，自組織にとってメリットであることを理解し，リスクに関する情報を共有する体制への参加を促すような制度設計が必要である。

CSIRT 導入による効果への期待をアンケート調査から示したが，さらなる普及促進に向けての課題を明らかにする必要がある。どのような要因が，組織における CSIRT 導入の推進要因，阻害要因となっていくかを明らかにし，セキュリティ対策を進めていくためのボトルネックの存在を明らかにしていきたい。

注

1）https://www.e-stat.go.jp/stat-search/files?page＝1&toukei＝00400001&tstat＝000001011528

2）https://www.nii.ac.jp/service/upload/sp-sample-2017.pdf

謝辞

夏季の多忙な時期に，アンケート調査に協力いただいた方々に感謝申し上げる。なお，本研究は科研費17K03741の助成を受けたものである。

参　考　文　献

菊池修，谷本茂明［2011］“CSIRTにおける組織形成に要するコスト構造定量化の検討,”プロジェクトマネジメント学会2011年度秋季研究発表大会予稿集，pp. 227-232.

見目悠平，谷本茂明，菊池修，杉浦芳樹，佐藤周行，金井敦［2013a］“CSIRTにおける人的資源管理方式に関する研究,”プロジェクトマネジメント学会2013年度秋季研究発表大会予稿集，pp. 105-110.

見目悠平，谷本茂明，菊池修，杉浦芳樹，佐藤周行，金井敦［2013b］“情報セキュリティマネジメントにおける保証レベルに関する検討,”プロジェクトマネジメント学会2013年度秋季研究発表大会予稿集，pp. 308-313.

小川賢［2018］“CSIRTの導入と組織内での情報の非対称性の影響に関する理論的考察,”神戸学院大大学経営学論集，Vol. 14，No. 2，pp. 55-68.

小川賢［2017］“大学におけるクラウド利用の阻害要因に関する分析,”日本経営システム学会誌　Vol. 34，No. 1　pp. 29-36.

小川賢［2015］“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,”神戸学院大学経営学論集　Vol. 11，No. 2，pp. 19-41.

島成佳，安藤玲未，高木大資［2015］“情報漏えいにつながる行動に関する実証分析,”情報処理学会論文誌，Vol. 56，No. 12　pp. 2191-2199.