情報セキュリティ対策自己点検・評価
ー結果分析とその活用についてー

立命館大学　情報システム部
岡　潤也

平成25年度　大学情報セキュリティ研究講習会

目次

Ⅰ　はじめに

（1）自己点検チェックリストの趣旨と成り立ちについて

・より適正な情報管理（大学の社会的責任のひとつ）を遂行するために、
情報資産の様態を体系的に把握し、弱点の発見と改善を期すもの。

・情報セキュリティ関連の事件事故における手口の多様さ、影響の甚大さ
を認識し、経営執行部含めたガバナンスの強化を期するもの。

・このような期待と危機意識のもと、
私情協における長年の研究と関係者の知見を踏まえて作成されたもの

Ⅰ　はじめに

（2）設問について

以下の4セクション、約80の設問で構成されています。

1. 情報資産の把握
　　保有資産目録、重み付け. . .
2. 組織的対応
　　意思決定ルール、セキュリティポリシー . . .
3. 人的対応
　　利用者把握、責任明確化. . .
4. 技術的・物理的対応
　　機器（ネットワーク・サーバー・PC）、媒体、施設. . .

※それぞれの設問意図と行動例（対策例）について私情協HPにて公開中。

Ⅰ　はじめに

（3）集計にあたって

配点について

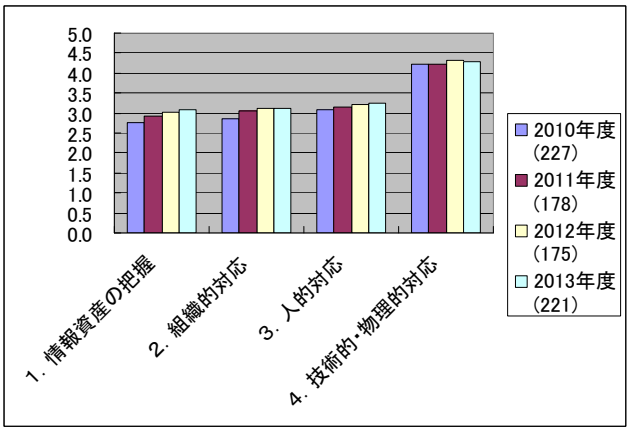
対応している	①本チェックリストの方法で対応	５点
	②本チェックリスト以外の方法での対応	５点
	③一部（部門・項目）対応している	４点
対応していない	④具体的に計画している	３点
	⑤必要性を感じており、これからの課題	１点
	⑥必要性を感じていない	０点

大学グループについて

ｸﾞﾙｰﾌﾟ	回答校数	概要
A	15大学	大規模大学　入学定員3,000人以上　複数学部有り
B	18大学	中規模大学　入学定員2,000人以上3,000人未満　複数学部有り
C	30大学	中から小　入学定員2,000人未満　複数学部あり、自然科学系学部有り
D	61大学	中小規模　入学定員2,000人未満　複数学部あり、自然科学系学部無し
E	7大学	自然科学系　単科大学
F	15大学	社会科学系　単科大学
G	8大学	人文科学系　単科大学
H	6大学	医･歯･薬系　単科大学
I	7大学	その他　単科大学
併設短大	52短大	大学併設短期大学
短大法人	2短大	短期大学法人

Ⅱ　自己点検結果概要

（1） 過去4年間の経年変化



- 全体的に右肩上がり もしくは横ばい。
- 2011年度に回答校数が減少、2013年度増加に転じるが同じ傾向を維持。
- 技術対応。物理対応は2011年代より4点台。

	2010年度 (227)	2011年度 (178)	2012年度 (175)	2013年度 (221)
１．情報資産の把握	2.8	2.9	3.0	3.1
２．組織的対応	2.9	3.1	3.1	3.1
３．人的対応	3.1	3.2	3.2	3.3
４．技術的・物理的対応	4.2	4.2	4.3	4.3

⇒改善が進みにくい分野？

Ⅱ．自己点検結果概要

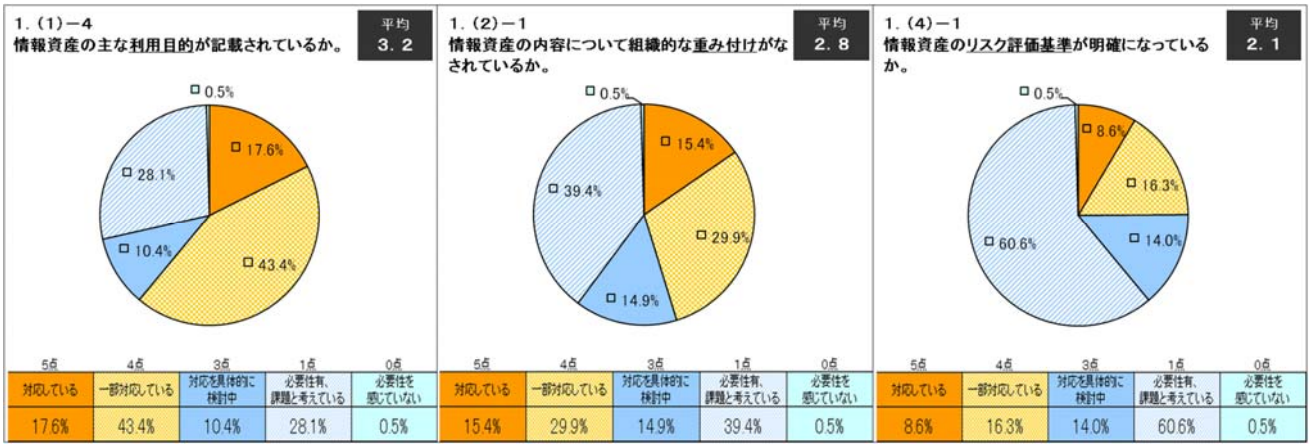
（2） 学校グループ別平均点および前年度比較

	A (15大学)	B (18大学)	C (30大学)	D (61大学)	E (7大学)	F (15大学)	G (8大学)	H (6大学)	I (7大学)	大学全体 (167大学)	併設短大 (52短大)	短大法人 (2短大)	短大全体 (54短大)
1．情報資産の把握	3.5	3.4	3.1	3.0	3.3	2.4	2.9	2.8	3.2	3.1	3.1	3.9	3.1
2．組織的対応	3.6	3.3	3.2	3.1	3.8	2.4	3.0	3.1	3.0	3.1	3.0	4.1	3.0
3．人的対応	3.7	3.4	3.3	3.2	3.9	2.5	3.1	3.1	3.2	3.3	3.2	4.2	3.2
4．技術的・物理的対応	4.5	4.4	4.3	4.4	4.3	4.0	4.5	4.0	4.4	4.3	4.1	4.9	4.2
合計	3.8	3.6	3.5	3.4	3.8	2.8	3.4	3.3	3.5	3.4	3.4	4.3	3.4

	A	B	C	D	E	F	G	H	I	大学全体	併設短大	短大法人	短大全体
1. 情報資産の把握	-2%	6%	5%	-3%	8%	3%	-4%	11%	6%	2%	-3%	17%	-3%
2. 組織的対応	1%	0%	0%	-4%	9%	4%	0%	18%	11%	1%	-6%	4%	-5%
3. 人的対応	3%	-1%	3%	-2%	11%	4%	-2%	13%	6%	2%	-5%	-6%	-5%
4. 技術的・物理的対応	-2%	1%	1%	-1%	1%	-3%	3%	4%	4%	0%	-5%	-1%	-5%
合計	0%	1%	2%	-2%	6%	1%	1%	10%	6%	1%	-5%	2%	-4%

Ⅲ．留意項目

「1．情報資産の把握」



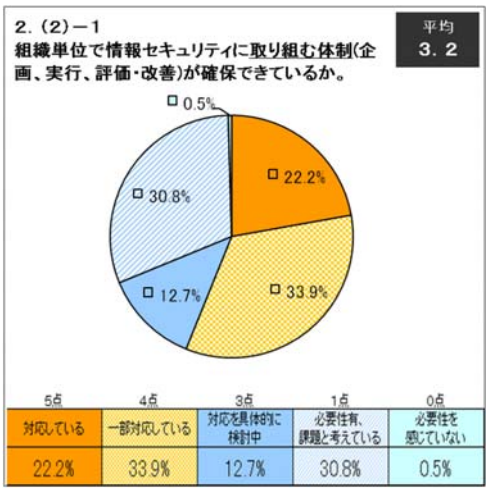
⇒目的外利用（特に個人情報）に起因する事故を防ぐためにも

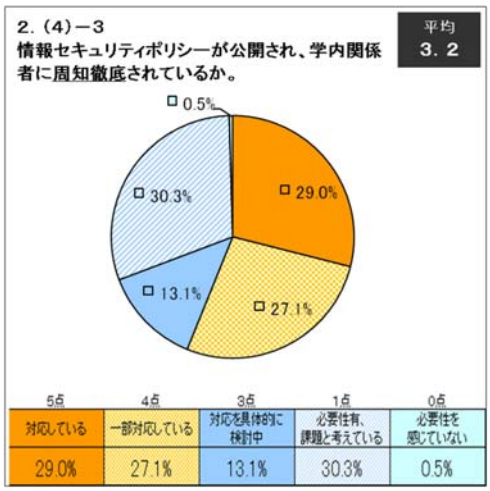
⇒現実的に管理を進める上でのプライオリティを明らかに

⇒データの重要性だけではなくシステムの脆弱性にも考慮を

Ⅲ. 留意項目

「2. 組織的対応」



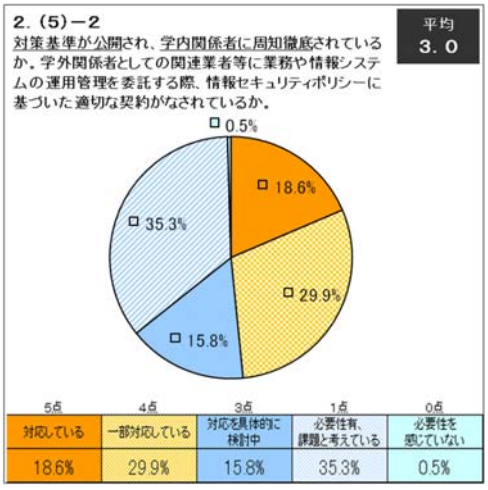


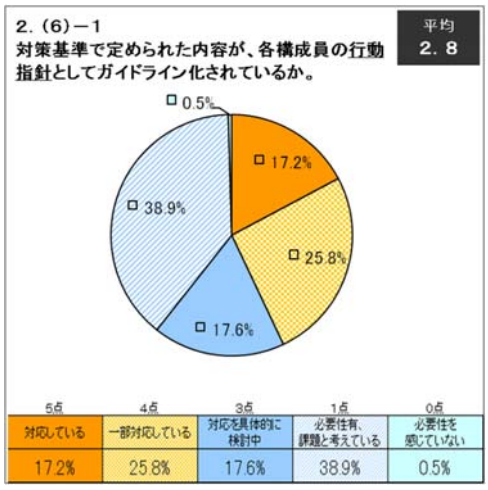
⇒日進月歩の技術確信(＝突破手口)に備えるためのPDCAサイクルを設ける

⇒策定が目的ではなく、周知実効を。(策定のしんどさを越えて、、、)

Ⅲ. 留意項目

「2. 組織的対応」





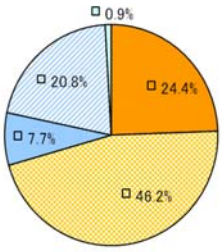
⇒システムに携わる「全関係者」が意識しなければセキュリティは守れない。

⇒より実践的な理解を深める必要がある。(頭では分かっていたが、、、では遅い)

Ⅲ. 留意項目

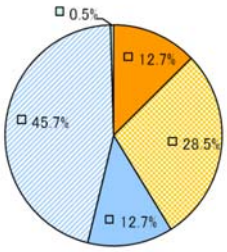
「3. 人的対応」

3.（2）
構成員に対して、セキュリティに対する問題意識を職務責任の中で明確にしているか。
平均 3.5



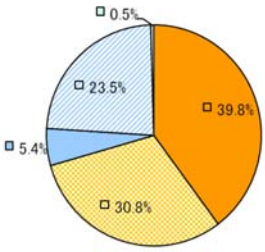
5点	4点	3点	1点	0点
対応している	一部対応している	対応を具体的に検討中	必要性有、課題と考えている	必要性を感じていない
24.4%	46.2%	7.7%	20.8%	0.9%

3.（7）－2
情報セキュリティ教育は定期的に実施され、参加を促す工夫がなされているか。
平均 2.6



5点	4点	3点	1点	0点
対応している	一部対応している	対応を具体的に検討中	必要性有、課題と考えている	必要性を感じていない
12.7%	28.5%	12.7%	45.7%	0.5%

3.（8）－1
事故の連絡体制、事故処理の責任体制が確立されているか。
平均 3.6



5点	4点	3点	1点	0点
対応している	一部対応している	対応を具体的に検討中	必要性有、課題と考えている	必要性を感じていない
39.8%	30.8%	5.4%	23.5%	0.5%

⇒モラルやマナーの問題ではなく、職責としての受け止めが必要

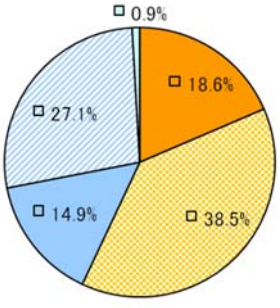
⇒絵に描いたモチではなく、理解・実践される工夫が必要

⇒「情報」「IT」であったとしても、他と同様、責任は生じる。

Ⅲ　留意項目

「4. 技術的・物理的対応」

4.（4）－2
情報媒体はパスワード設定や暗号化等の紛失・盗難対策を講じているか。
平均 3.1



5点	4点	3点	1点	0点
対応している	一部対応している	対応を具体的に検討中	必要性有、課題と考えている	必要性を感じていない
18.6%	38.5%	14.9%	27.1%	0.9%

⇒小型で個人が所持せざるを得ない媒体の管理が最な困難のひとつ。万一、紛失があった場合でも次善の策を用意しておく。

Ⅳ　まとめ

・情報セキュリティ対策の必要性が理解され、年々対策が改善されつつありますが。いっぽうで守るべき裾野、攻撃手口の多様さ、社会から期待される役割も拡大の一途をたどっています。

・一過性のルール策定や研修活動、システム実装にとどまらず、絶え間無いPDCAの継続や新たな事象への対応が求められています。

・近年重みを増してきた事象のひとつに「サイバー攻撃対策」や「災害復旧対策」があげられますが、本年7月の私情協での調査によると多くの大学がその必要性を感じながらも、まだまだ実践には移れていません。

・情報セキュリティ対策は「忙しく」「辛い」取り組みですが、大学間で協力し合うことで更なる底上げやキャッチアップも期待できます。本日この後のプログラムでも、実践に向けたテーマを設ける予定です。

おわり

ご清聴ありがとうございました。