マネジメントシステムの
情報セキュリティ版がもたらすもの
―信頼？姿勢？安心？―

徳島大学・情報センター
上田哲史

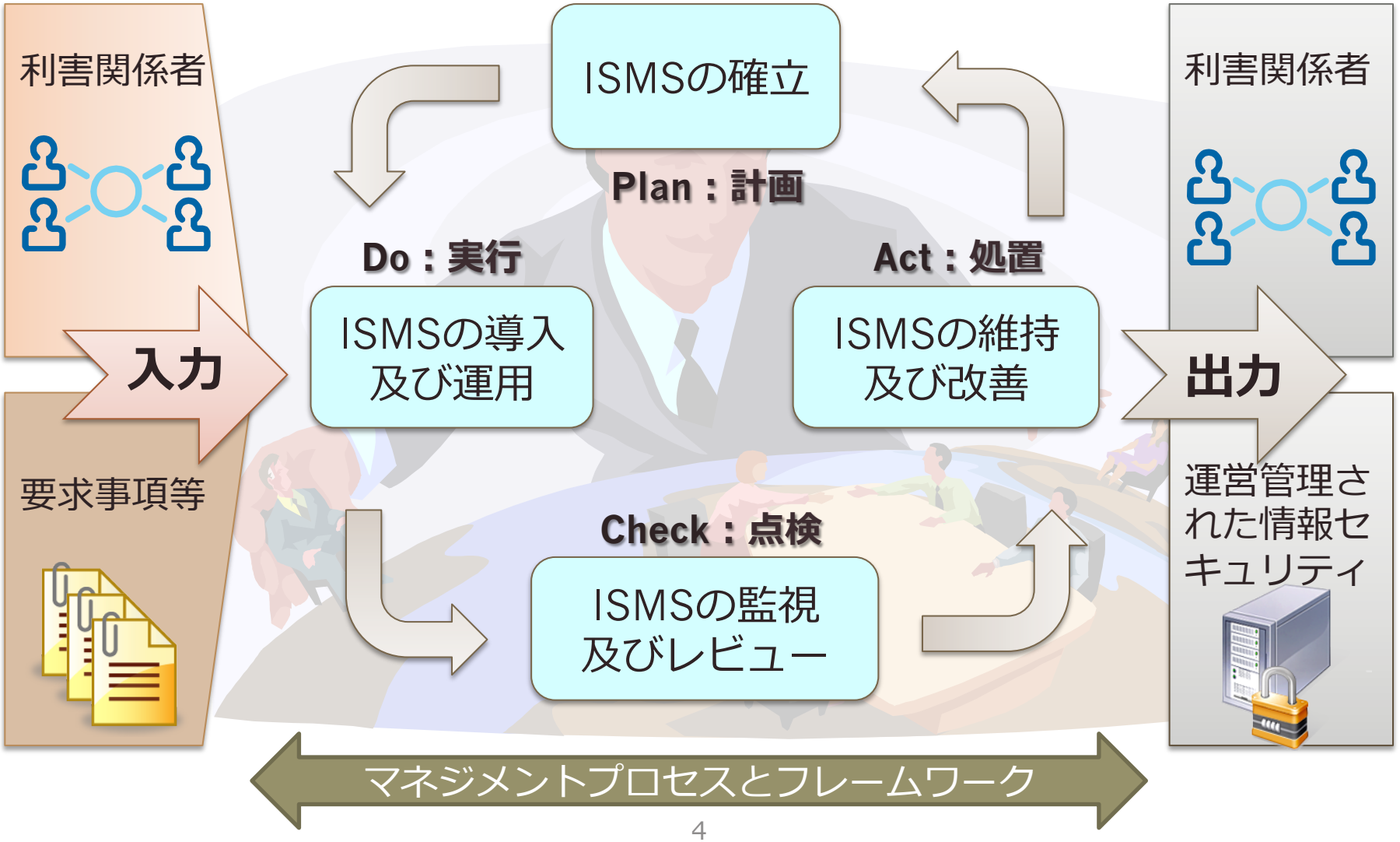
徳島大・情報センターのご紹介

- 理系（医歯薬，工，総合科学） 5 学部
  - 学部 5,900人　大学院 1,600人
  - 教員 960人，事務職員＋技術職員 1,300人
  - 合計約1万人　（徳島市人口：約26万人）
- 情報センター沿革
  - S41 電子計算機センター
  - S58 情報処理センター
  - H 6 総合情報処理センター
  - H14 高度情報化基盤センター
  - H22 情報化推進センター　←　**H24 ISMS 取得**
  - H26 情報センター
- 情報センターの目的
  - 大学全体の情報システム・サービスの統括的管理（事務系も含む）

マネジメントシステム

- 生産・品質管理
- 「組織が方針及び目標を定め、その目標を達成するためのシステム」に関する規格
- **PDCAサイクル**を回して向上させていく
  - P: Plan; 計画
  - D: Do; 実施・実行
  - C: Check; 点検・評価
  - A: Act; 処置・改善
  - PDCA→PDCA とスパイラルアップ
- 環境 ISO14000 series, 品質 ISO9000 series

ISMSのPDCAサイクル



さっそくのクリッカー質問

ISMSを組織で導入をされている，もしくは導入検討をされていますか？

1. 導入している
2. 導入を現在検討している
3. 導入を検討した結果，やめた
4. 導入予定はない

何故ISMS導入を検討するのか？

- 何らかのよい噂を聞いたので
- 情報セキュリティは抜かり無くやっとかないと…
- ISOの枠組みと似てるらしいから
- 保険相当
- **連携先・取引先がISMS取得を要求している**
- 情報セキュリティ対策の見える化

日本のISMS取得大学

登録番号	組織名称	所在地	取得年月日	認定機関
IC03J0027	国立大学法人 静岡大学（情報基盤センター）	静岡県	2003年11月25日	ISR007
IS 90359	学校法人　日本福祉大学	愛知県	2005年3月16日	ISR004
IS 509958	早稲田大学（メディアネットワークセンター）	非公開	2007年1月24日	ISR004
I165	国立大学法人宇都宮大学（総合メディア基盤センター）	栃木県	2007年11月15日	ISR002
IS 523803	学校法人日本大学（総合学術情報センター）	非公開	2007年12月4日	ISR004
IC08J0241	国立大学法人山口大学	山口県	2008年10月24日	ISR007
IC11J0338	**国立大学法人徳島大学（情報化推進センター）**	徳島県	2012年3月9日	ISR007
IS 582429	国立大学法人九州大学（情報統括本部）	福岡県	2012年3月22日	ISR004
IS 590859	国立大学法人長崎大学	長崎県	2013年3月4日	ISR004
JUSE-IR-289	国立大学法人 鹿児島大学（学術情報基盤センター）	鹿児島県	2013年4月23日	ISR005
IS 601919	国立大学法人岡山大学（情報統括センター）	岡山県	2013年11月12日	ISR004
I327	国立大学法人横浜国立大学（情報基盤センター）	神奈川県	2014年3月6日	ISR002

静岡大学

項目	内容
組織名称	国立大学法人 静岡大学
組織部門名称	情報基盤センター
所在地	静岡県静岡市駿河区大谷836
認証基準	JIS Q 27001:2006(ISO/IEC 27001:2005)
認証登録番号	IC03J0027
登録範囲	学内ネットワークおよび各種情報基盤サービスの管理･運営･提供ならびに学術ネットワークハブ拠点の管理･運営
適用宣言書	静大情セ-ISMS- 2009年9月15日発行
初回登録日	**2003年11月25日**
有効期限	2015年11月24日
認証機関	株式会社日本環境認証機構(JACO)

山口大学

全学が範囲
長崎大学と類似

項目	内容
組織名称	国立大学法人山口大学
組織部門名称	－
所在地	山口県山口市吉田1677-1
認証基準	JIS Q 27001:2006(ISO/IEC 27001:2005)
認証登録番号	IC08J0241
登録範囲	1．基幹ネットワークシステムの管理運用 2．大学情報機構が提供する教育・研究用コンピュータの管理運用 3．学内業務情報システムの運用支援 4．修学支援システムサーバの管理運用
適用宣言書	国立大学法人山口大学ISMS適用宣言書（口大情環 第20号、2013/7/3）
初回登録日	2008年10月24日
有効期限	2014年10月23日
認証機関	株式会社日本環境認証機構(JACO)

九州大学

項目	内容
組織名称	国立大学法人九州大学
組織部門名称	情報統括本部
所在地	福岡県福岡市東区箱崎6-10-1
認証基準	JIS Q 27001:2006(ISO/IEC 27001:2005)
認証登録番号	IS 582429
登録範囲	**1.情報環境整備推進室が提供する情報サービス** **2.情報システム部・情報企画課・事務ICT支援グループが提供する業務システムサービス**
適用宣言書	2012年3月15日付適用宣言書 第3版
【他の事業所】	1)馬出病院キャンパス 2)伊都キャンパス
初回登録日	2012年3月22日
有効期限	2015年3月21日
認証機関	BSIグループジャパン株式会社

センターは
入ってない！

徳島大学

項目	内容
組織名称	国立大学法人徳島大学
組織部門名称	情報化推進センター
所在地	徳島県徳島市南常三島町2-1
認証基準	JIS Q 27001:2006(ISO/IEC 27001:2005)
認証登録番号	IC11J0338
登録範囲	全学情報ネットワークシステムの運用管理、ハウジング・ホスティングシステムの運用管理、教育用システムの運用管理及び専門技術アドバイスサービス
適用宣言書	ISMS-B06-D04 2011/11/25
初回登録日	2012年3月9日
有効期限	2015年3月8日
認証機関	株式会社日本環境認証機構(JACO)

Why ISMS?

- 体制作り／維持
- セキュリティ活動の可視化
- Public Relation
- 認証取得を保険とみなす

ISMSの効果―端的にいうと

- ベネッセ事件がありました
- 凄まじい数の顧客情報が流出
- ベネッセ子会社のシンフォームが顧客情報の管理をしていた
- 犯人は，シンフォームへ派遣されたSE
- シンフォームはISMSを取得していた

さあ，どう思います？？

国立大がISMSを取る意義

- クラウド利用には不可欠
- セキュリティポリシー等に応じた人的・技術的・環境物理的セキュリティ対策が明確にされる
- 情報資産が洗い出され，組織の責任境界が明らかにされる
- 経営層が関わり，セキュリティ対策にかける各コストが把握・承認され，組織ぐるみの取り組みとなる
- 規格が取れたことが広報(publicity)に資する
- **情報資産の大学間持ち合い**などに関して，互いを信頼するに足りる資格となる
- 外部評価等の対策が楽になる

組織としての最悪のケース

- 十分な技術的，環境・物理的セキュリティ対策が整備されていない
- 責任体制（人事構成や緊急時体制）が明確になっていない
- 事故時の緊急連絡・指示手順が無い（もちろん訓練もできていない）
- 適切な報告が上がって来ない⇒社会への説明がなされない
- 保険等に入っていない

■当然の帰結

- **社会的な非難**
- **信用失墜**，入学希望者減
- 事故対応に組織メンバーが疲弊
- 損害賠償など，組織として無意味な支出
- 保険に入りにくくなる？

宣伝：国立大学法人情報系センター協議会(NIPC) ISMS研究会

- 2011.07.15　第８回 IOT通算第14回研究会と合同開催（幹事校: 静岡大）
- 2012.03.15-16 第９回 IOT通算第16回研究会と合同開催（幹事校: 宇都宮大）
- 2012.09.13-14 第10回 第7回国立大学法人情報系センター研究交流・連絡会議／第16回学術情報処理研究集会と合同開催 （幹事校: 徳島大）
- 2013.09.09-10 第11回 第8回国立大学法人情報系センター研究交流・連絡会議／第17回学術情報処理研究集会と合同開催 （幹事校: 山口大）
- 2014.9.26-27 第12回　信州大にて予定

情報セキュリティ対策

- 技術的セキュリティ対策，環境・物理的セキュリティ対策では，**脅威への未然対応は限界がある**のは明らか…今回の会合のテーマ
- では，インシデント，アクシデントが発生したときは！

☞スマートな機械や仕組みが，
後始末をしてくれることはない

- **万が一の場合における組織防衛の担保は？？**

☞そんなものはありません

学長やCIOは謝罪がお嫌い

また，謝れば何とかなる問題ではなく…

・組織の信用失墜→入学者減，公募応募者減
・直接制裁→賠償など
・間接的制裁→運営交付金削減

一度押された烙印（レッテル）はなかなか剥がすことができない

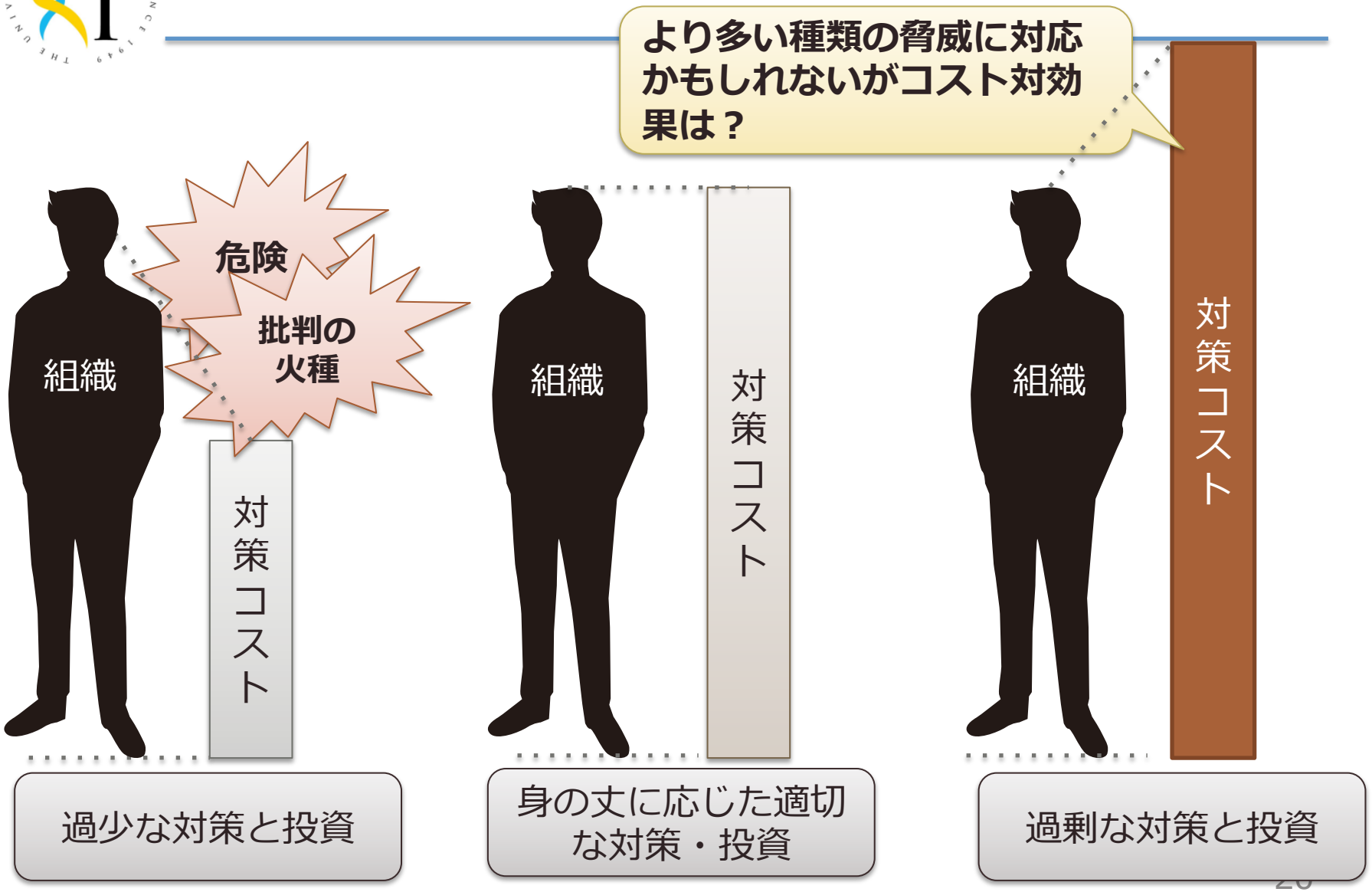
続いてのクリッカー質問

組織において情報セキュリティと言えば，どれにポイントを置かれますか？

1. ファイアウォールなど，水際での技術対策
2. アンチウィルス導入など，クライアント対策
3. サーバでのソフトウェア更新，コンテンツのチェック
4. 構成員に対するセキュリティ教育

※どれも大事です

対策の適切さ：費用対効果の観点



対策の適切さ

身の丈に応じた適切な対策・投資

ISMS: 組織の情報セキュリティ対策が「適切な対策・投資」となっているかを客観的に第三者が**評価・監査**する

規格の要求事項に対する対策の実装確認（適用宣言書の妥当性，およびその通り運用されているかどうか，規定・記録から判定）

情報セキュリティ３要素：CIA

- **機密性(Confidentiality)**
  - ある情報が許可された者にのみアクセスできる
  - 例：個人認証による保護
- **完全性(Integrity)**
  - プロセスが正確で改ざんされないこと
  - 例：デジタル署名，入力フォームのサニタイジング
- **可用性(Availability)**
  - 許可された者がある情報に随時アクセスできること
  - 例：SLAでの稼働率・遅延時間などの指定，維持

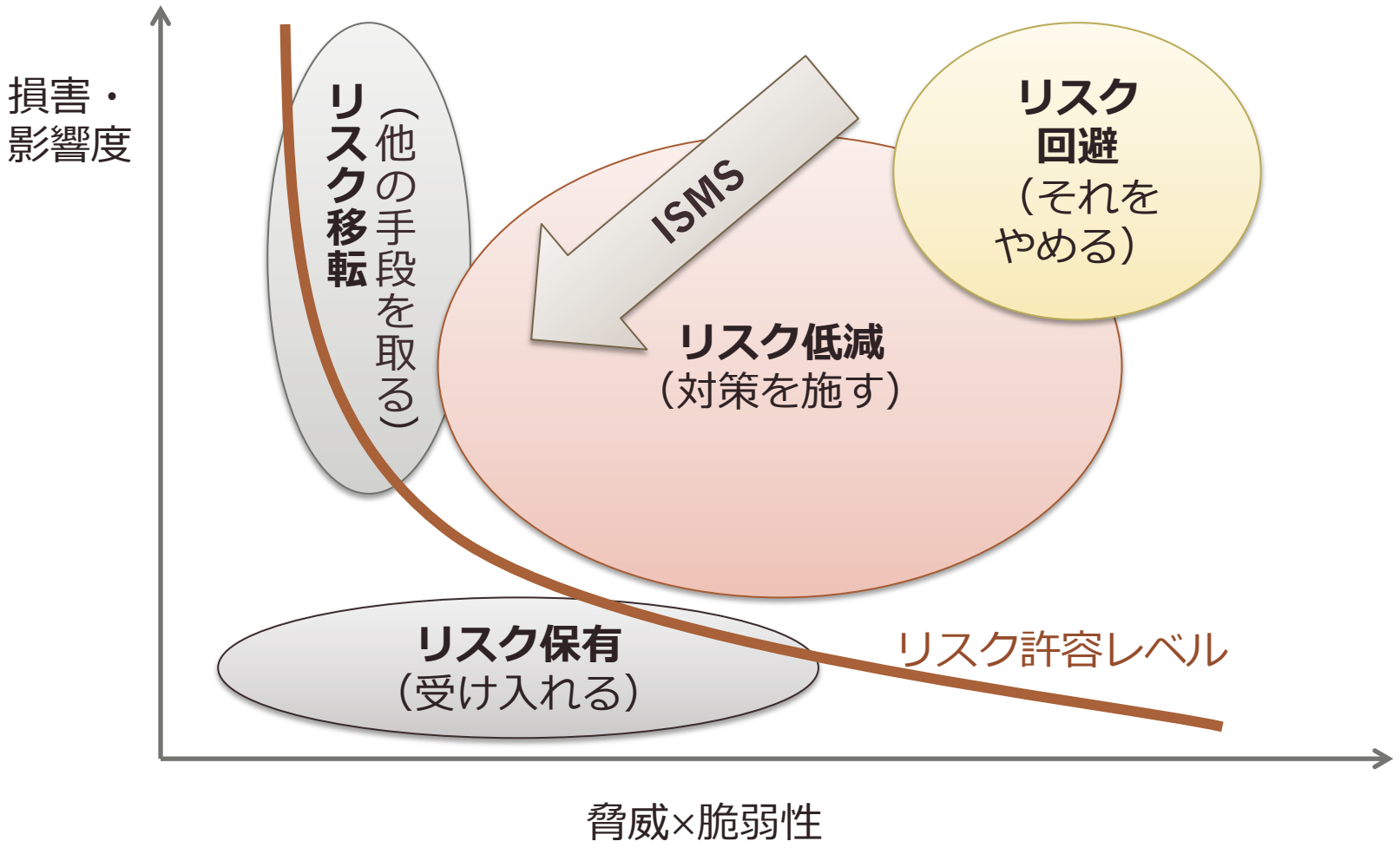
ISMS＝リスクマネジメント

- 情報資産について，CIAの観点からリスク値を評価し，それに応じた対策を行う
- **リスク値＝資産価値×脅威×脆弱性**
  - 資産価値：情報やシステムのCIA観点における重要度
  - 脅威：原因とその頻度
  - 脆弱性：脅威の発生に対する頑健度
- 一次元のリスク値という数値に応じて，通常は**リスク対応策**を講じる
  - リスク低減，リスク移転，リスク回避，リスク受容によりリスク値を下げる

情報資産の洗い出し，リスク分析

- 業務に関する情報システム，情報，情報機器を漏れなくリストアップ
- BYODも意識（業務に用いるなら対象情報機器とすべし）
- CIAの観点からリスク値を算出
  - 重要性：どの種類の情報が重要かを定義する
  - 脆弱性：盗難，改ざんなど典型例アリ
  - 脅威：影響度を定義する
- リスク受容値以上であれば，**リスク対応計画**
  - 受容値内であっても管理

リスク対応


損害・
影響度
リスク移転
（他の手段を取る）
ISMS
リスク
回避
（それを
やめる）
リスク低減
（対策を施す）
リスク保有
（受け入れる）
リスク許容レベル
脅威×脆弱性

さまざまな困難

- リスク対応策が終わっても…
- 管理策は**133**ある
  - 取捨選択できるようにはなっているが，恐らく通常の大学運営であれば**ほとんど全部適用**せざるを得ない（徳島大学は**131**選択）
  - 「…しなければならない」という**絶対要求事項**に対してエビデンスとともに，**適用する理由**と対応する規定を示した表を，**適用宣言書**といい，ISMSのもっともキモの文書となる
  - 対策の有効性を測定しなければならない

事故

- 未知の脅威に堪えうる完璧な対策が無い
- しかし，ISMSの仕組みの実装，PDCAによる継続管理により，事故・事件の生起確率は，無策の場合に比して相当に低く抑えられる（はず）
  - その時点で考えうる限りの合理的な管理策・リスク対応策の集合であるISMSに合格した☞もっともらしい

- **それでも，事故は起こりうる**

事後

- 初期対応は迅速に行われないといけない
- 事後の検証も大切
  - 普段十分備えていた（管理策をとり，リスクを認識し，対策していた）
  - その備えようは恣意的，主観的ではなく，国際規格に沿って改善を続けていた

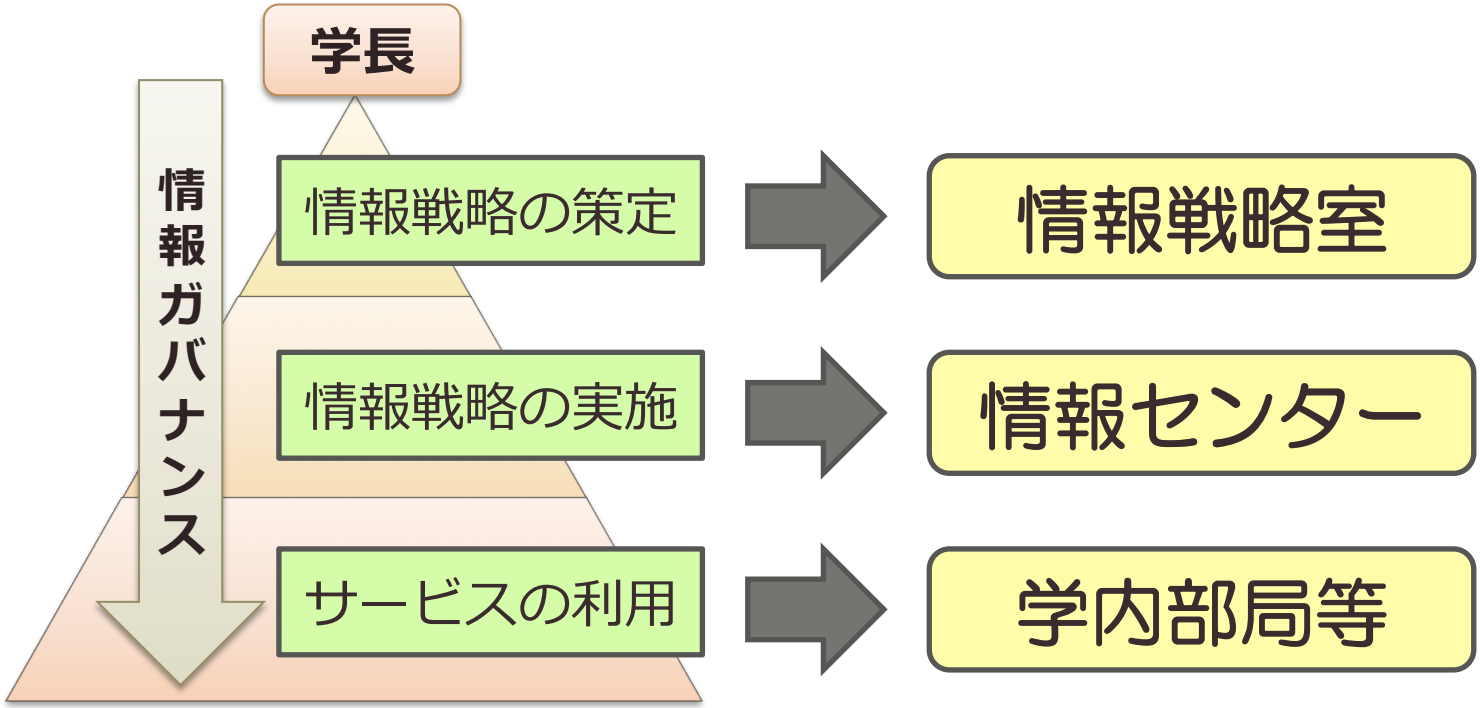
☞**構成員，父兄，ステークホルダ，社会**は「最大限努力していたのね，やむを得なかったのね」と理解してくれる（はずだ）

ISMSの本質

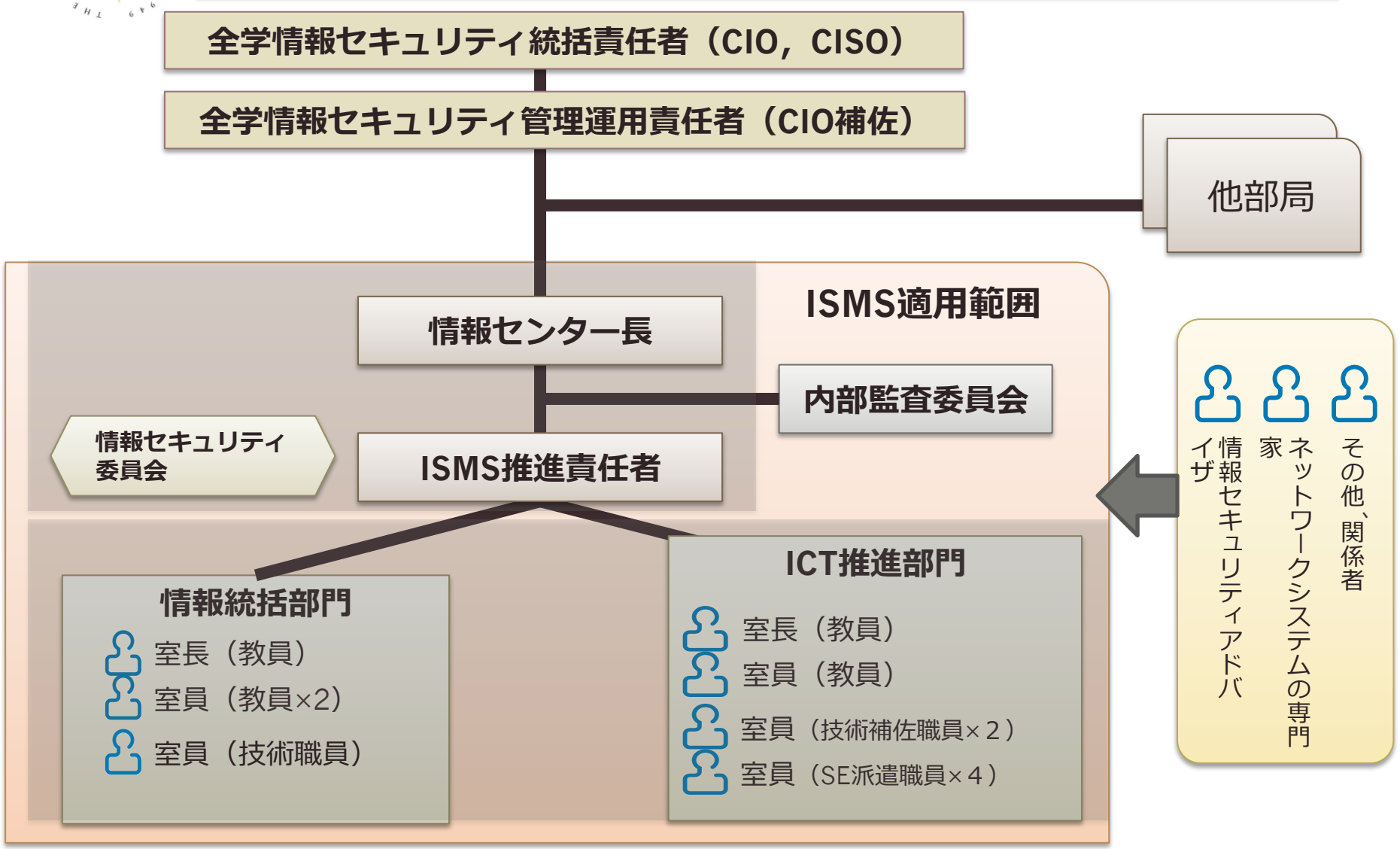
- 人的セキュリティ対策を策定
  - **性悪説に基づく規定と責任組織体制**作り
    - 組織の親規則に準拠し，管理規定を策定
    - 役職だけでなく委員会組織も構成
    - 内部監査組織，監査人も任命
    - 事故時の判断基準や連絡網整備が重要（ISMSとしてではなく組織としてもともと整備すべき）
  - 範囲，方針を決め
  - リスクマネジメント
    - 資産（価値）を洗い出し，それらに対して想定される脅威・脆弱性を評価
    - リスク値＝価値×脅威×脆弱性
    - そのリスク値の軽減策を策定

徳島大学の情報ガバナンス体制

- 学内の情報ガバナンスの強化



情報化推進センターのISMS推進体制



韓国セウォル号事故

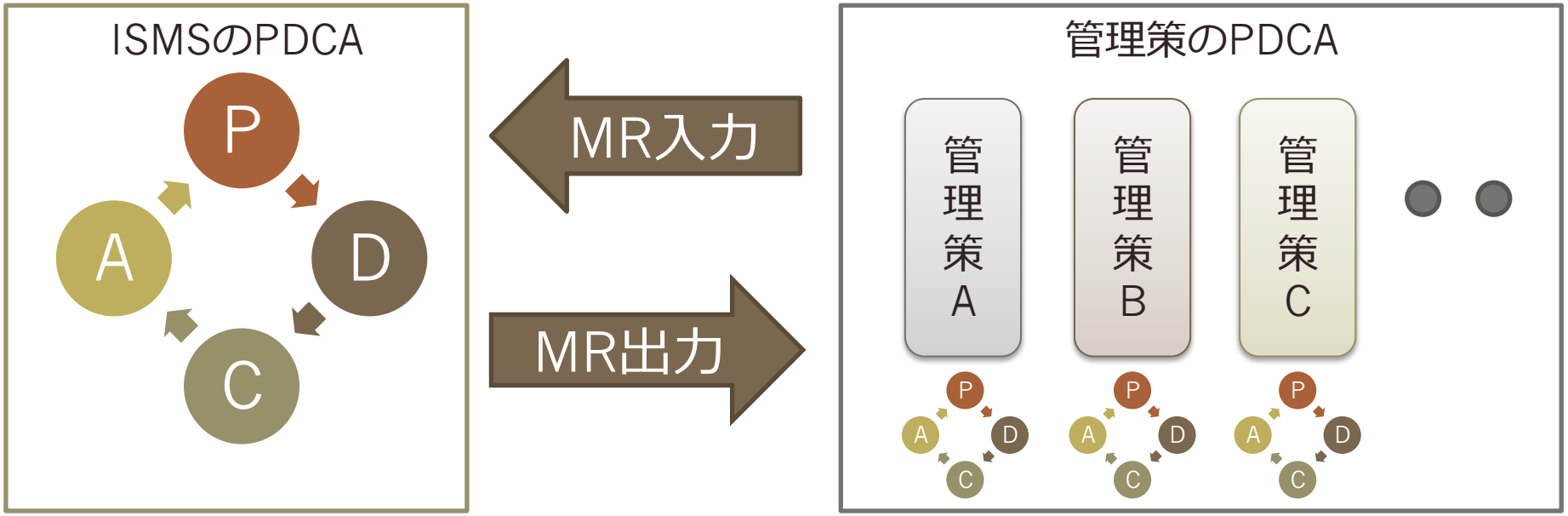
- 企業の**事業継続性**の観点
  - ルールや法令等に基づく平時の安全管理
  - 事故発生時の対応
  - 事故原因究明
- これらが全て不十分⇒社会的に非難を浴びる
- 企業（海運会社）そのものの事業はもはや**立て直し不可能**
  - 損害賠償
  - 信用失墜

ありあけ沈没事故(2009)

- セウォル号と類似の船舶に関する事故
  - 過積載ではなく，強い波を受けたため固定していた荷物が急激に移動した
  - 沈没したが全員無事（乗員・乗客数は少なかった）
    - 船員，船長による適切な誘導
    - 組織的な対応
- 平時に適切な対策が施され，（訓練による経験が活かされ）事故時も被害は最小限
  - **遵法**だったと社会に理解される⇒**誹りは最小限**
  - 恐らくは保険金も満額支払われたのではないか
  - 会社は**事業は継続できた**
- 国や業界はコンテナ固定に関する対策を強化
  - PDCAの成果

二重のPDCAサイクル

- ISMS全体を運用するためのPDCAサイクル
  - 内部監査、マネジメントレビュー(MR)等
- 各管理策についてのPDCA
  - 管理策毎の**有効性測定**/評価/改善等
  - MR結果、是正措置/予防措置等の要求により変化



もちろんお墨付きなど，実質ではない

- 性悪説的立場に沿って対策しているISO各規格
  - 監査日予告つきの定期監査は完璧ではない
  - 構成員の意識が「性悪」であればいくらでも抜け道
- 書類上の証左は表面的なものでしかなく，組織が一丸となって**「情報資産を護ろう」という意識作り**が必要
- **周知・教育は重要**

ベネッセ事件1/2

- ベネッセ社の下請けシンフォーム社に勤める派遣SEが，堅固なデータベースの脆弱性を突き，顧客情報を抜き取り，転売.
- シンフォームはISMSを取得していた
  - 通信・運用管理に職務の分割，開発・試験・運用の場所の分離やログ監視が規定されているはず
  - 管理策は有効であったのか？リスク分析がなされていたかどうかは調べられる
  - ISMS審査機関，認定機関の瑕疵も調べられることに

☞**恣意的な運営ではなかったのね，とは思われている**

☞**ISMSを取っていなければ…**

ベネッセ事件2/2

以下の批判にも耳を傾けて改善せねばならない

- 対策が有効なら漏洩するはずがなかった
- 相手先が認証を持っていたら警戒せずに取引というのも問題
- **情報漏えいが起きたときの責任逃れに認証取得が使われている**
- 認証審査が通れば、運用は形式化しがち

※PRESIDENT 2014/8/18号

結局，教育

- 教育の実施
  - 情報セキュリティの諸問題と対策の理解
  - ISMSの仕組みそのものの理解
    - **仕組みが出来ているから情報セキュリティ管理ができるのではない**
    - 情報セキュリティを管理するために仕組みを導入し，目標を設定し，達成・改善してゆく
- 教育の効果測定
  - 力量測定と併せて
  - 気づきなどを通してPDCAに構成員が貢献する奨励

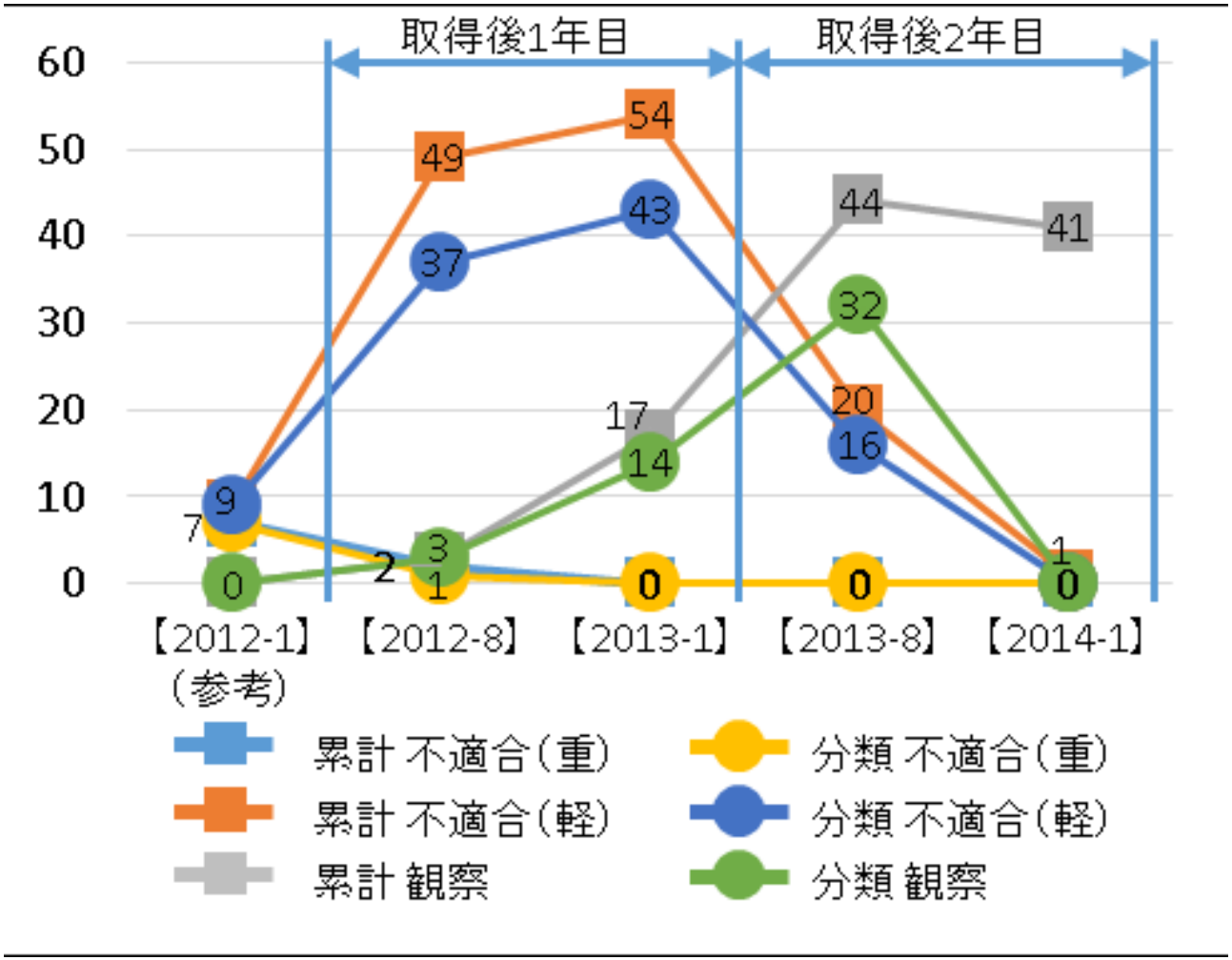
転換期

- 今までは…
  - CISOはあて職だったかもしれない
- 今後は…
  - 大学ではインターネット＋コンピュータはどんどん運営・経営に食い込んでくる（退潮は無い）
  - クラウド利用は不可避（むしろ積極利用）なので，情報セキュリティポリシー，情報ガバナンス，ISMSを束ね，判断・指示・**予算確保**できる人物が必要
  - 国立は特に概算要求等，国に対策費用を求めることは今後は困難⇒運営交付金から定常予算に組込む

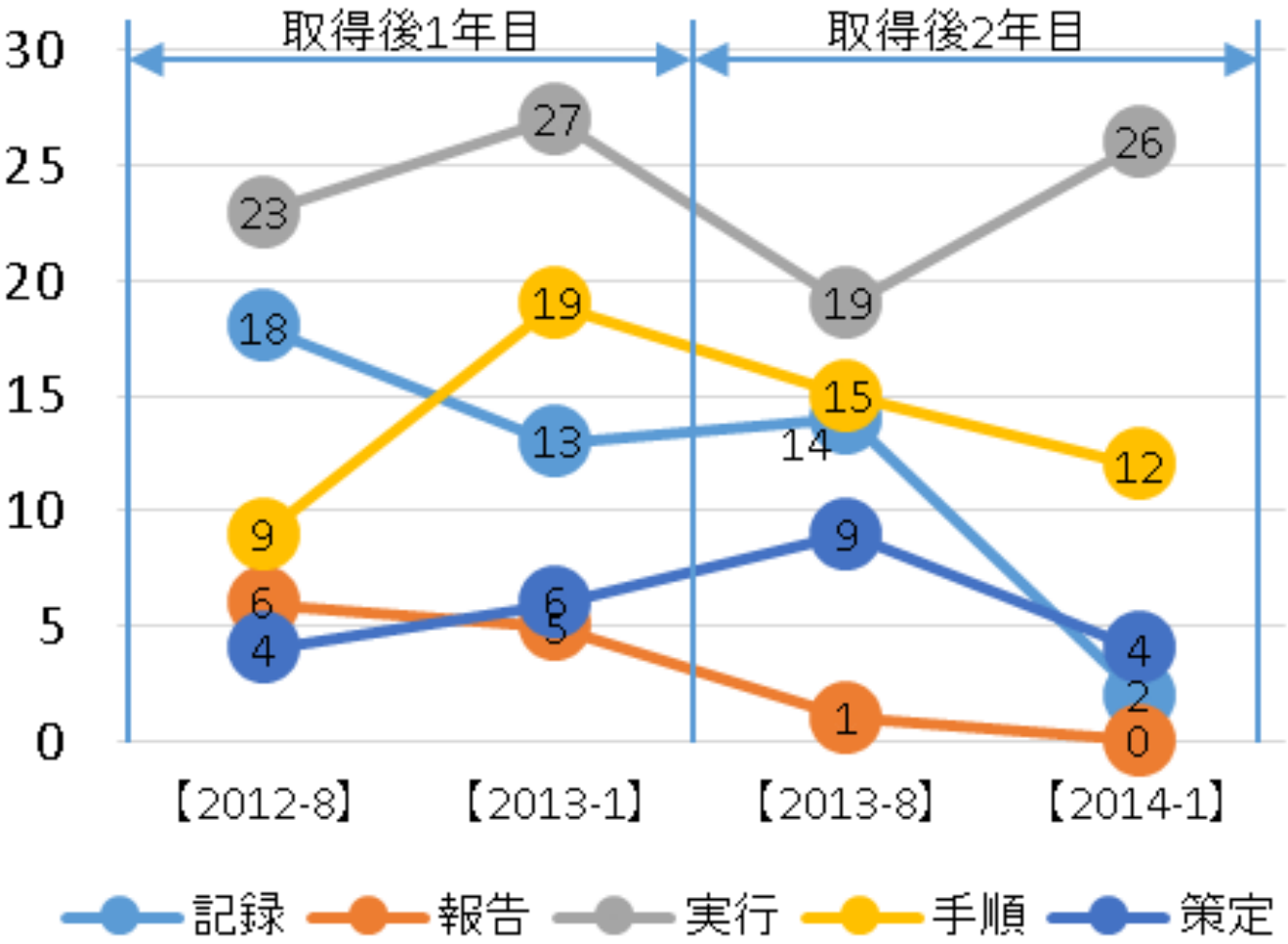
ISMS取得の効果は？徳島大の場合

- 良い点
  - 曖昧だった業務プロセスの明確化、業務手順の見直し
  - 様々な**問題点を可視化**
  - 職員の意識の変化
  - 学内外に対してのアピール
- 苦労した（している？）点
  - 業務プロセスの明確化
  - 情報資産の洗い出し，リスク評価
  - 記録！
  - 派遣職員の教育
- 導入後の課題
  - 課題は山積、PDCAの継続で改善を！

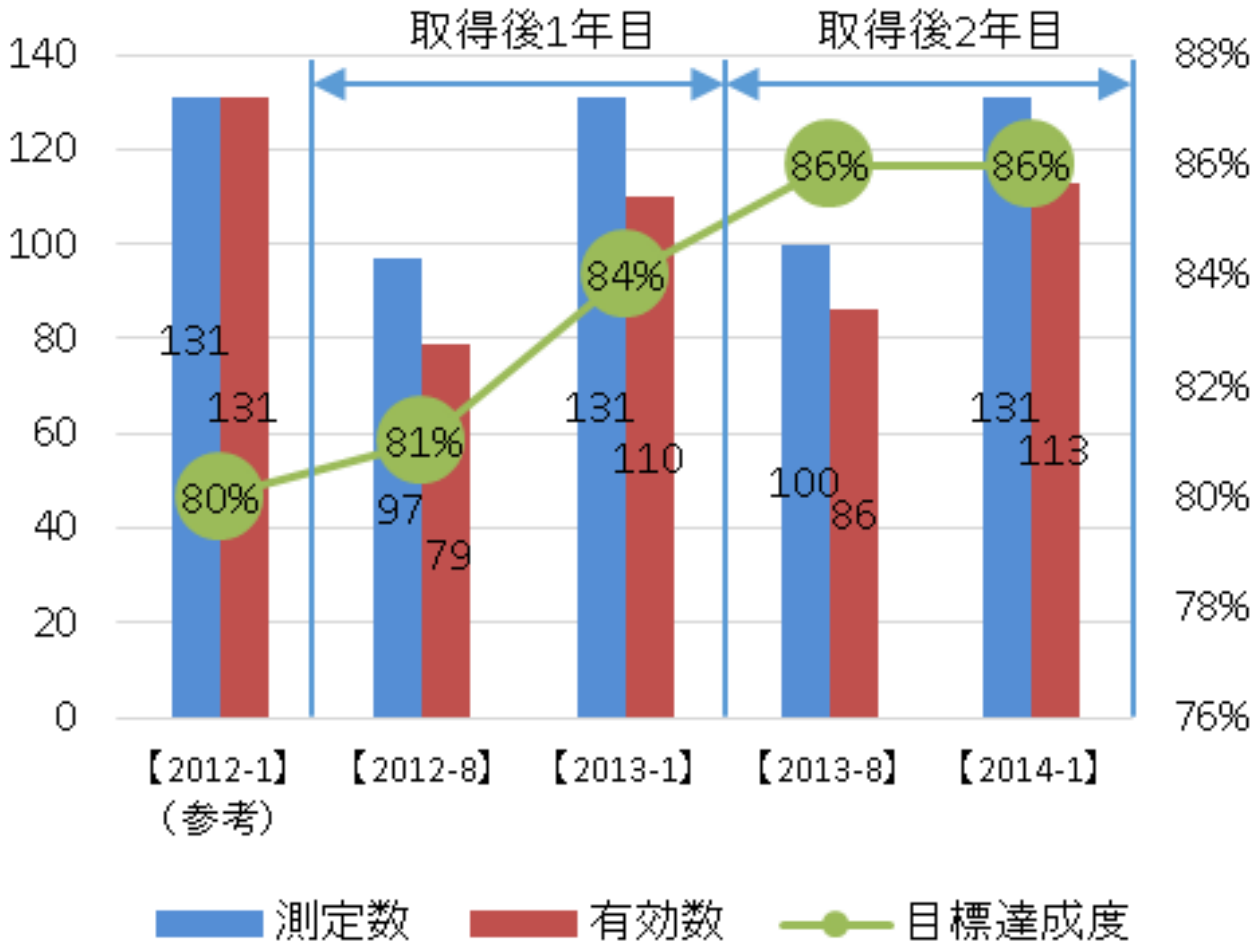
内部監査指摘数累計


取得後1年目
取得後2年目
60
50
40
30
20
10
0
54
49
44
43
41
37
32
20
17
16
14
9
7
3
2
1
0
0
0
1
0
【2012-1】
(参考)
【2012-8】
【2013-1】
【2013-8】
【2014-1】
累計 不適合(重)
累計 不適合(軽)
累計 観察
分類 不適合(重)
分類 不適合(軽)
分類 観察

内部監査分類別指摘数


取得後1年目
取得後2年目
30
25
20
15
10
5
0
27
23
26
19
19
18
15
13
14
12
9
9
6
6
5
4
4
1
2
0
【2012-8】
【2013-1】
【2013-8】
【2014-1】
記録
報告
実行
手順
策定

有効性評価達成率


取得後1年目
取得後2年目
140
120
100
80
60
40
20
0
88%
86%
84%
82%
80%
78%
76%
131
131
80%
97
79
81%
131
110
84%
100
86
86%
131
113
86%
【2012-1】
（参考）
【2012-8】
【2013-1】
【2013-8】
【2014-1】
測定数
有効数
目標達成度

ISMS取得2,000事業所への調査

1. 効果について『**セキュリティ意識が従業員に浸透した**』や『**情報資産が明確になり整理できた**』という回答が上位
2. 一般の情報セキュリティ調査に比べて本調査対象組織はマルウェアへの感染率が半分程度であり、認証取得は情報セキュリティ対策実質化に効果があると思われる
3. コンサルタントや審査員に対しては全般的に不満など，受審者からは厳しい評価がある
4. 審査員やISMS推進担当者等の考えに、「リスクマネジメント」概念の理解が不足している感じ

※星，畑上，内田「ISMS認証取得組織のアンケート調査からみる現状と課題」日本セキュリティマネジメント学会全国大会，2011.

ISMS維持は損か得か？

- 費用
  - 初期費用100万円，年間50万円程度
  - パブリシティ効果　＜　体制維持の客観的評価
- 手間
  - 定常時：記録を残す「くせ」をどうつけるか
    - 自動集計や定期サーベイでルーチン化，効率化
  - 非常時：BCP規定やマニュアルが効力発揮
  - 審査時：段取りは慣れるとできるようになる

終わりに

- 情報セキュリティ対策に「完全なる技術パッケージ」が出現し得ない限り，ISMSの存在感は大きい
- 事件・事故のほとんどはヒトがやってしまうので，ヒトの性悪説的管理，人的セキュリティ対策は必須
- ISMS自体がなんらかの保険として機能しうるかどうかは「ISMSの実質運用」にかかっている