システム技術分科会　選出
システム技術分科会 2014 年度第 1 回会合 より

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？―

上田 哲史
(徳島大学)

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
ueta@tokushima-u.ac.jp

平成 26 年 8 月 25 日

近年，ISMS を取得する大学が増加している．その背景にはパブリシティの価値もあるが，本質的には大学組織がこれまであまり意識していなかった情報ガバナンスの構築に関して，ISMS が本質的に適切な仕組みであること，また，今後クラウド利用が促進するにつれクローズアップされるであろう事件事故災害に対する BCP, 人的体制維持，セキュリティ教育普及など，ISMS の PDCA に包含されている魅力などがある．

本学では 2012 年 3 月に，国立大学としては 4 番目に ISMS を取得した．現在は 3 年目 (認証期間最終年度) となっている．ISMS の枠組みは情報センターの運営そのものに直接反映され，また，取り組みの全てが，情報ガバナンス体制維持，セキュリティ対策予算策定，外部評価，改組，クラウドによる情報システム最適化などに結びついてきている．発表ではそれらの概要を述べるとともに，ISMS が果たす人的セキュリティ対策の効果について，本学の状況を示す．なお，配布資料には一部発表内容が削除されている．

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

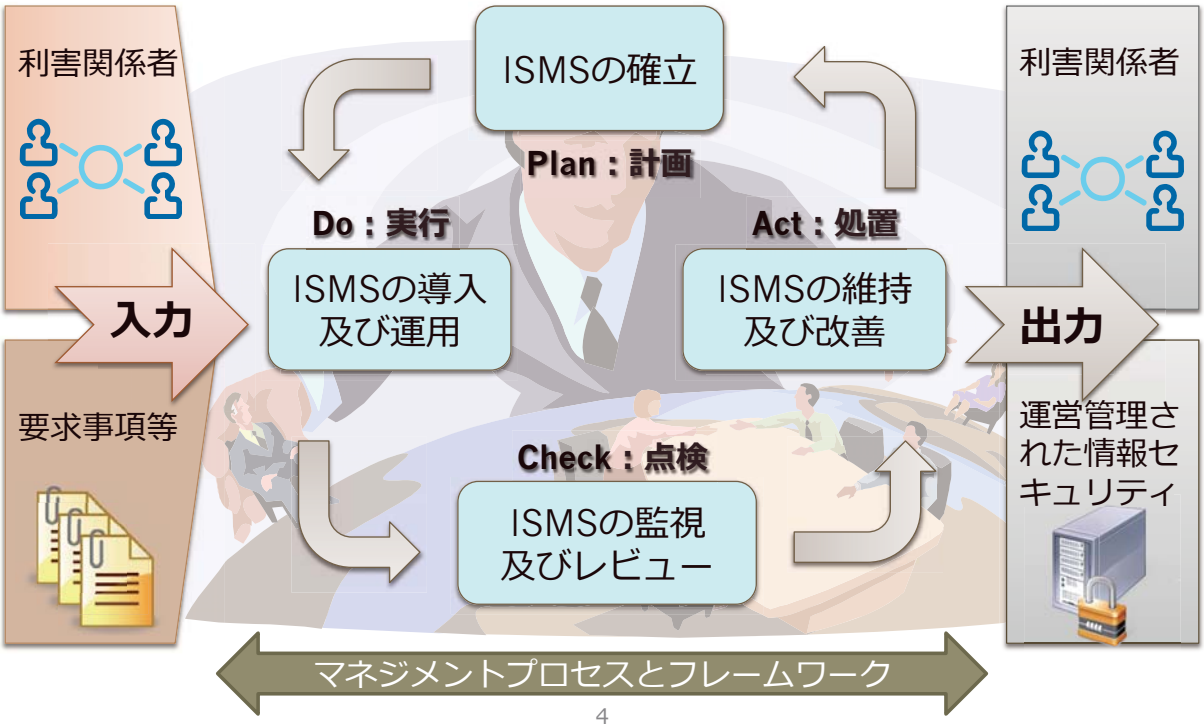
徳島大・情報センターのご紹介

- 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

センターは
入ってない！

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

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

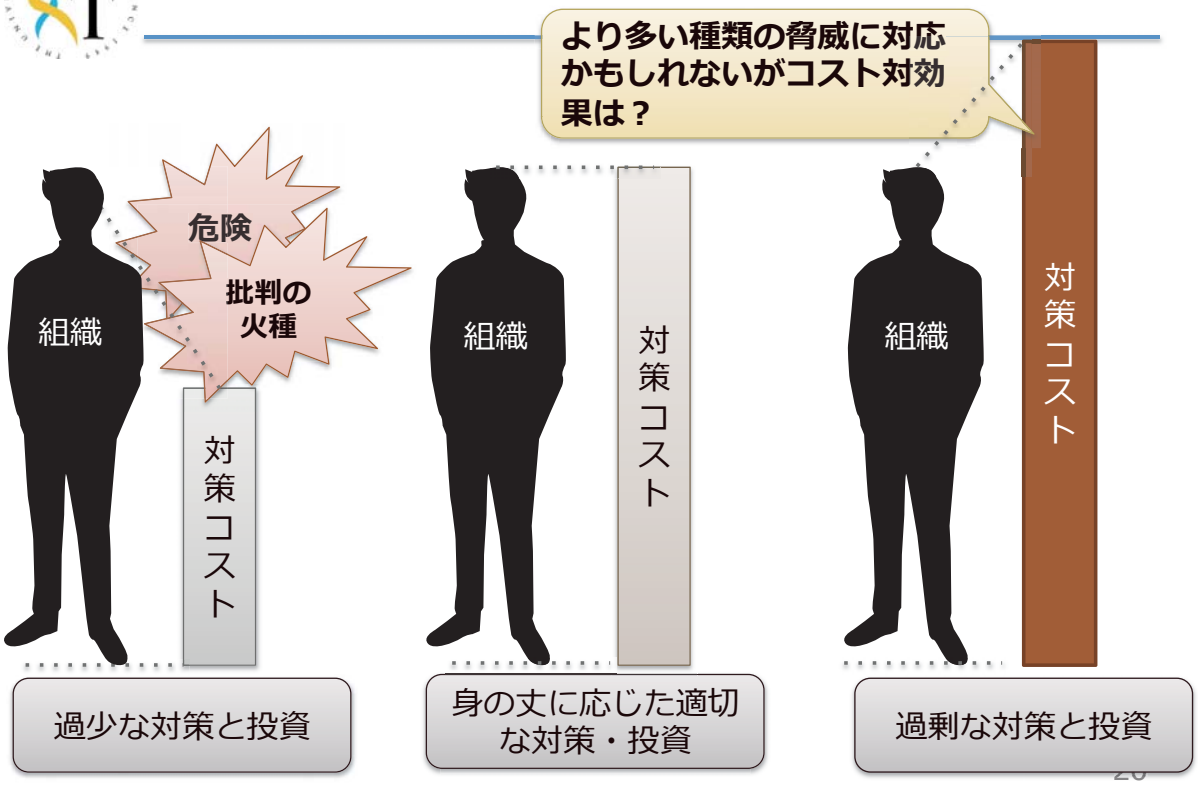
続いてのクリッカー質問

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

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

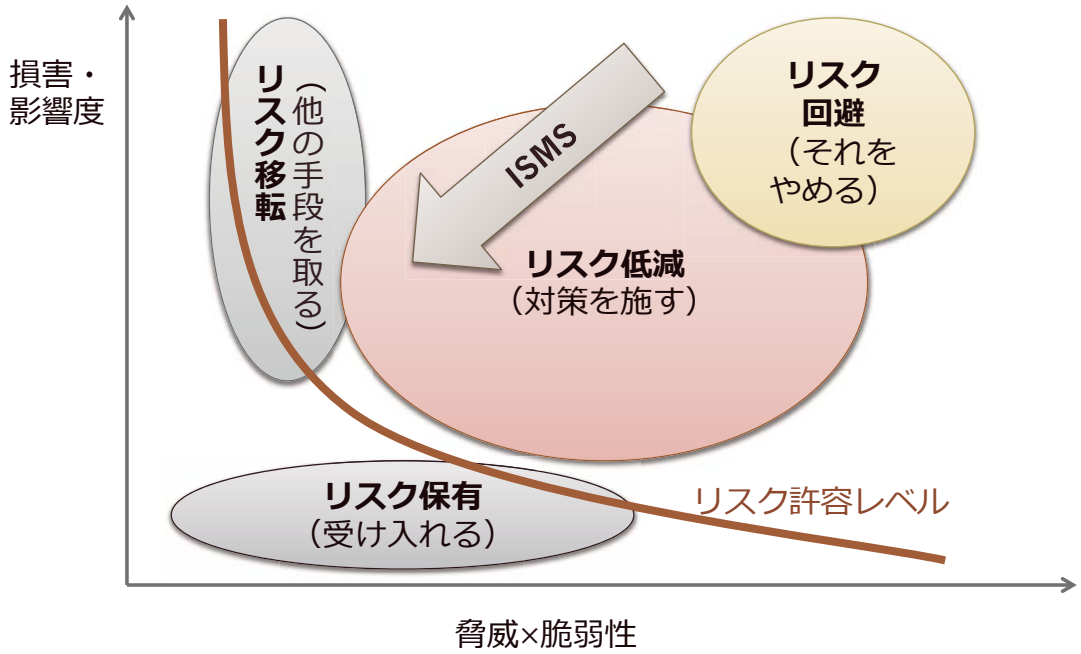
ISMS＝リスクマネジメント

- 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



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

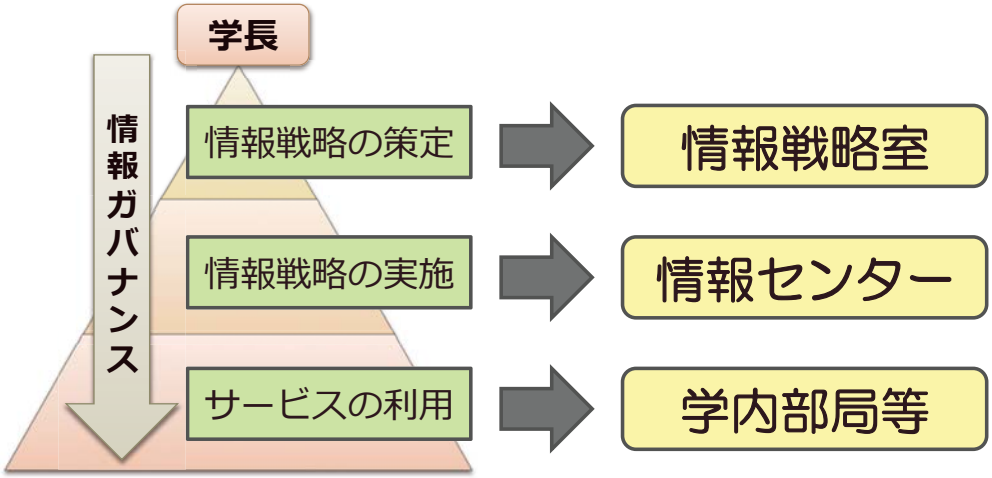
☞**構成員，父兄，ステークホルダ，社会**は「最大限努力していたのね，やむを得なかったのね」と理解してくれる（はずだ）

ISMSの本質

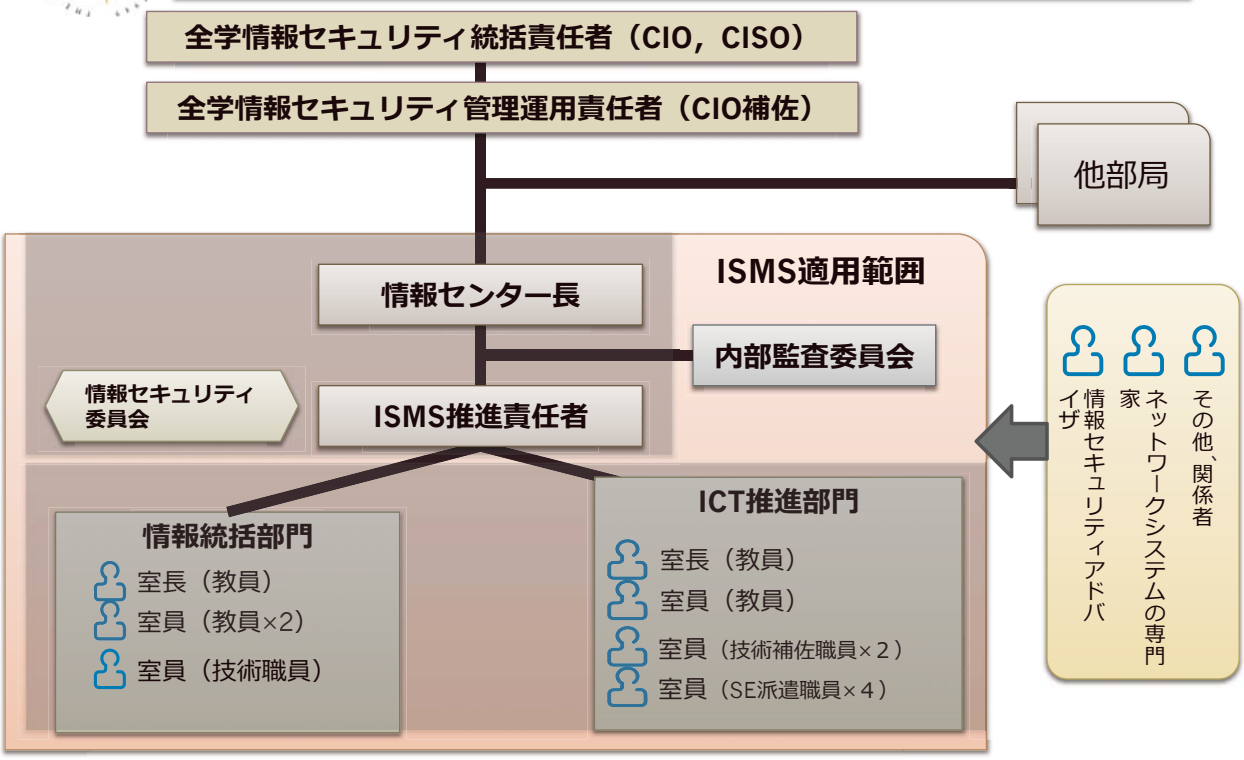
- 人的セキュリティ対策を策定
  - **性悪説に基づく規定と責任組織体制**作り
    - 組織の親規則に準拠し，管理規定を策定
    - 役職だけでなく委員会組織も構成
    - 内部監査組織，監査人も任命
    - 事故時の判断基準や連絡網整備が重要（ISMSとしてではなく組織としてもともと整備すべき）
  - 範囲，方針を決め
  - リスクマネジメント
    - 資産（価値）を洗い出し，それらに対して想定される脅威・脆弱性を評価
    - リスク値＝価値×脅威×脆弱性
    - そのリスク値の軽減策を策定

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

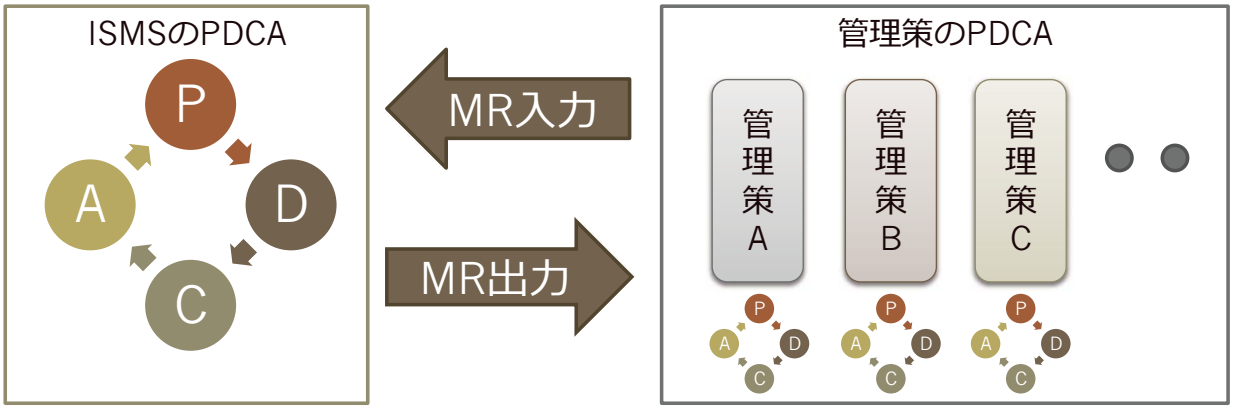
- 企業の**事業継続性**の観点
  - ルールや法令等に基づく平時の安全管理
  - 事故発生時の対応
  - 事故原因究明
- これらが全て不十分⇒社会的に非難を浴びる
- 企業（海運会社）そのものの事業はもはや**立て直し不可能**
  - 損害賠償
  - 信用失墜

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

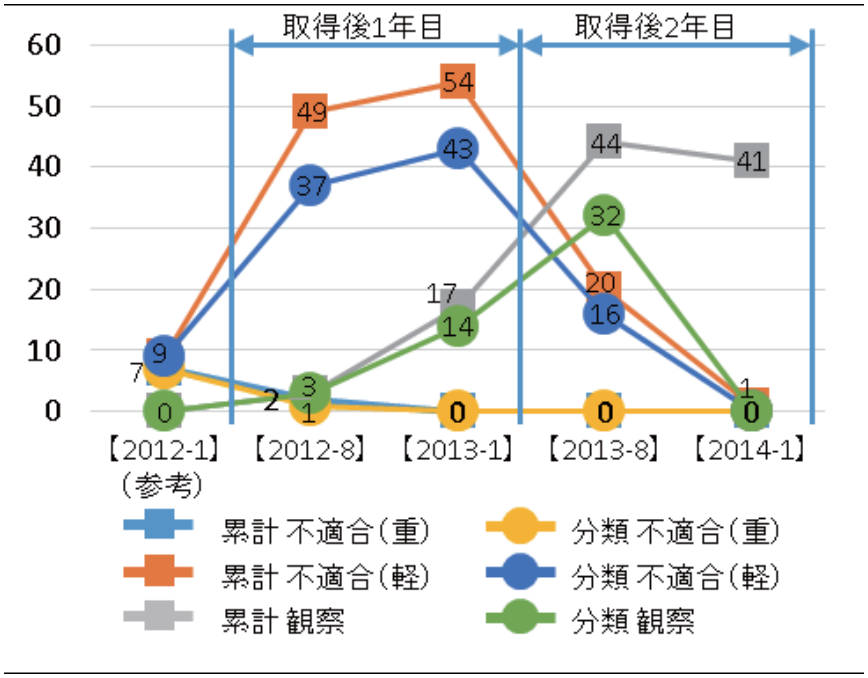
転換期

- 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

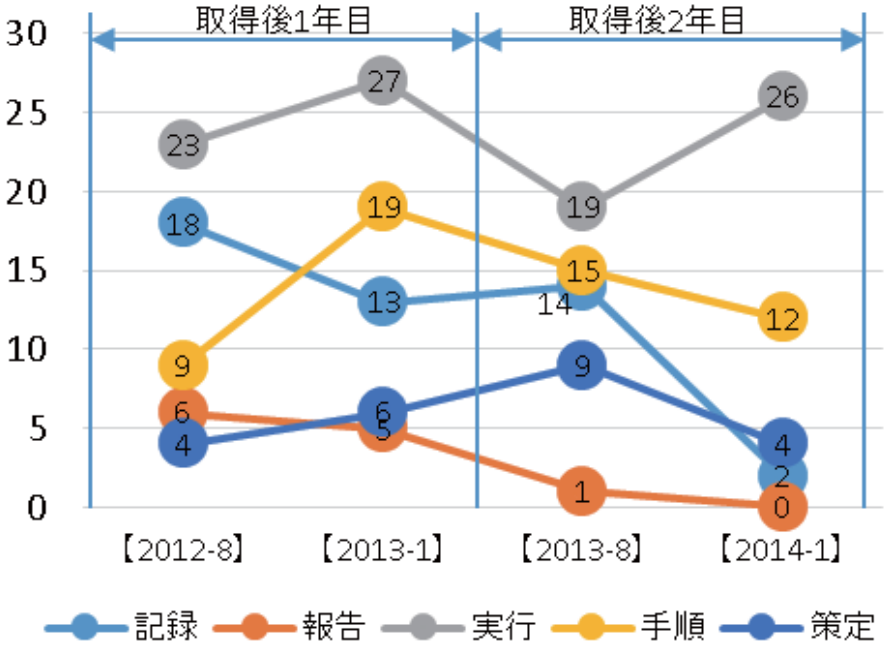
ISMS取得の効果は？徳島大の場合

- 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！

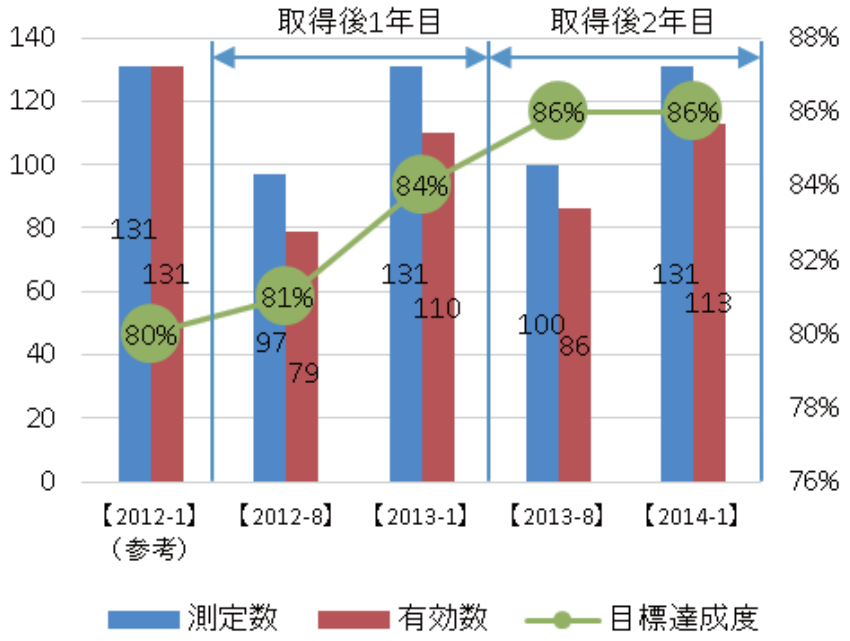
内部監査指摘数累計



内部監査分類別指摘数



有効性評価達成率



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

システム技術分科会　選出
システム技術分科会 2014 年度第 2 回会合 より

学内情報基盤のネットワーク管理の法的側面と最新動向

高橋 郁夫
(駒澤綜合法律事務所)

学内情報基盤のネットワーク管理の法的側面と最新動向

髙橋郁夫

1　問題点

大学における学内情報基盤については、その運営面についても、一定の整備が進んでいる。クラウドコンピューティングの発展・普及、社会一般の情報化の進展、ネットワーク接続形式の多様化およびそれに伴う管理の多様化などの情報技術の発展は、その運営をめぐる問題についても、いろいろな観点から新しい問題を提起している。これらの問題を法的な観点から整理するのが、本講演の目的となる。

2　具体的な対応

2.1　クラウド技術の発展および普及

ネットワークの具体的な運用に際して、情報セキュリティ対策のための規定は、サンプルなどが公表されており、それらに基づいて対応がなされているものと考えられる。しかしながら、近時は、クラウド技術の発展および普及により、そのリスクをどのように判断し、運用の際に従来の仕組みを新しい技術として取り入れるかということが問題になっている。クラウドを利用するといえども、その基本は、リスクの分析とその評価・軽減等の対策である。そのような形から、従来のネットワーク運用のポリシを見直す必要がある。

2.2　社会一般の情報化の進展

ネットワーク利用に関する問題行為等にたいする大学の対応等に関して大学の責任問題の議論がさらに議論されるようになってきている。大学の設置する掲示板における名誉棄損発言に関する大学の責任問題や学内ネットワークの不正使用による外部への不正アクセスに関する大学の責任などの問題である。一般論としては、個別・具体的な事案において管理に関して具体的な過失があるかどうかの問題になる。単にアクセスしうる立場を提供していただけで責任を問われることはない。

2.3　ネットワーク接続の多様化に伴う問題

現在、学内に携帯電話の基地局が設置されたり、学内の無線 LAN のアクセスポイントに携帯電話事業者を相乗りさせたりということがなされるようになってきている。これらの場合に、業として電気通信事業を営む者として、登録／届け出をなさなければならないのかという問題がある。これについては、詳細なマニュアルがあるが、電気通信事業自体で利益を上げようとする場合には、登録・届け出の対象になることに留意する必要がある。

また、多様化するネットワーク接続に対応して、ネットワーク管理も複雑多様化している。そのなかで、具体的な通信についての管理をなす場合には、通信の秘密との関係で、具体的な同意が必要になることに留意が必要である。もっとも、この同意の具体性については、まだ、明確ではないところである。

学内情報基盤のネットワーク管理の法的側面と最新動向

駒澤綜合法律事務所
高橋郁夫

本日の話題

- 大学でのネットワーク運用に関する法律的な側面の整理
- 具体的な事例に対する法律面での考え方
- 背景
  - ネットワーク運用が当然に
  - 特にクラウドの活用
  - 無線・携帯電話回線の利用

大学におけるネットワーク運用と法律の側面

- 大学のネットワーク運用と法律
  - ネットワーク運用ガイドラインについて
  - ネットワーク管理について
    - 通信の秘密との関係
    - 個人情報保護法との関係について
    - 情報セキュリティの維持の義務
    - 著作権侵害について
    - ゼミの掲示板等での名誉毀損について
    - 大学のネットワーク利用による攻撃

クリッカー　1

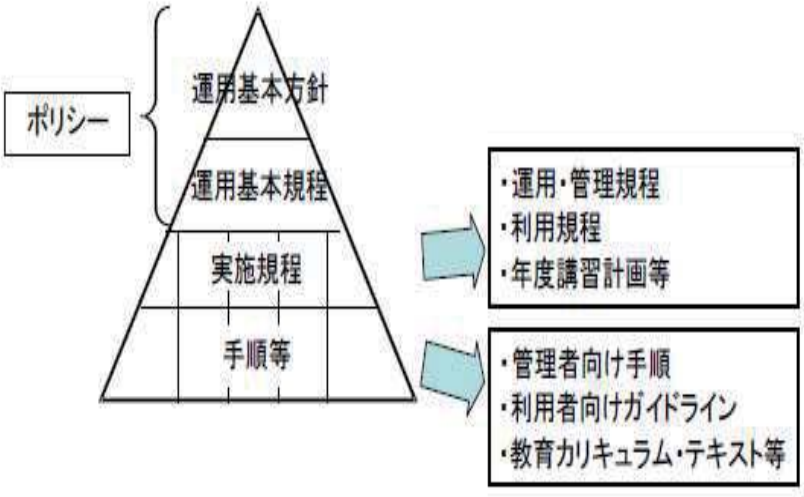
- 「高等教育機関の情報セキュリティ対策のためのサンプル規程集」について
- １　よく知っている
- ２　だいたい知っている
- ３　名前だけは知っている
- ４　知らない

ネットワーク運用ガイドラインについて

- 高等教育機関におけるネットワーク運用ガイドライン
  - (http://www.ieice.org/jpn/teigen/nwgl.html)
- 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
  - (http://www.nii.ac.jp/csi/sp/doc/sp-sample-2013.pdf)

質問1：大学では、クラウドを大規模に導入して、アカウント管理・学生の管理の事務まわりに利用しようと考えています。
このようなクラウドを導入するのにあたって、特に考えておく事項はあるのでしょうか。
海外のクラウドを利用していた場合に、何か問題がおきたときに、どこの裁判所でどのような問題が判断されるということになるのでしょうか。

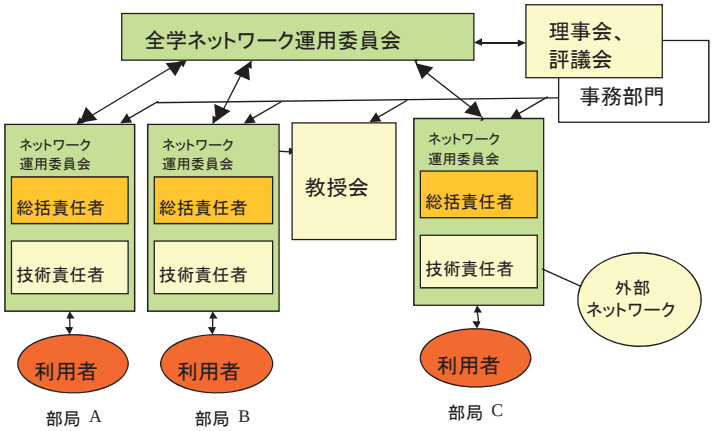
サンプル規定集(ポリシー)の位置づけ



ポリシー	実施規程	手順・ガイドライン等
B1000 情報システム運用基本方針 B1001 情報システム運用基本規程	B2101 情報システム運用・管理規程 B2102 情報システム運用リスク管理規程 B2103 情報システム非常時行動計画に関する規程 B2104 情報格付け基準	B3100 情報システム運用・管理手順の策定に関する解説書 B3101 情報システムにおける情報セキュリティ対策実施手順（策定手引書） B3102 例外措置手順書 B3103 インシデント対応手順 B3104 情報格付け取扱手順 B3105 情報システム運用リスク評価手順 B3106 人事異動の際に行うべき情報セキュリティ対策実施手順 B3107 機器等の購入における情報セキュリティ対策実施手順（策定手引書） B3108 外部委託における情報セキュリティ対策実施手順 B3109 外部委託における情報セキュリティ対策に関する評価手順
	B2151 情報セキュリティ要件の明確化に関する技術規程 B2152 情報セキュリティ対策に関する技術規程 B2153 情報システムの構成要素に関する技術規程	B3151 セキュリティホール対策計画に関する様式（策定手引書） B3152 ウェブサーバ設定確認実施手順（策定手引書） B3153 電子メールサーバのセキュリティ維持手順（策定手引書） B3154 ソフトウェア開発における情報セキュリティ対策実施手順（策定手引書）
	B2201 情報システム利用規程 B2202 認証基盤利用規程	B3200 情報システム利用者向け文書の策定に関する解説書 B3211 学外情報セキュリティ水準低下防止手順 B3212 自己点検の考え方と実務への準備に関する解説書
		B3251 情報機器取扱ガイドライン B3252 電子メール利用ガイドライン B3253 ウェブブラウザ利用ガイドライン B3254 情報発信ガイドライン B3255 利用者パスワードガイドライン
	B2301 年度講習計画	B3300 教育テキストの策定に関する解説書 B3301 教育テキスト作成ガイドライン(利用者向け) B3302 教育テキスト作成ガイドライン(システム管理者向け) B3303 教育テキスト作成ガイドライン(CIO/役職者向け)
	B2401 情報セキュリティ	B3401 情報セキュリティ監査実施手順

人的なシステムについて

- CIO、運用部門、技術サポート部門



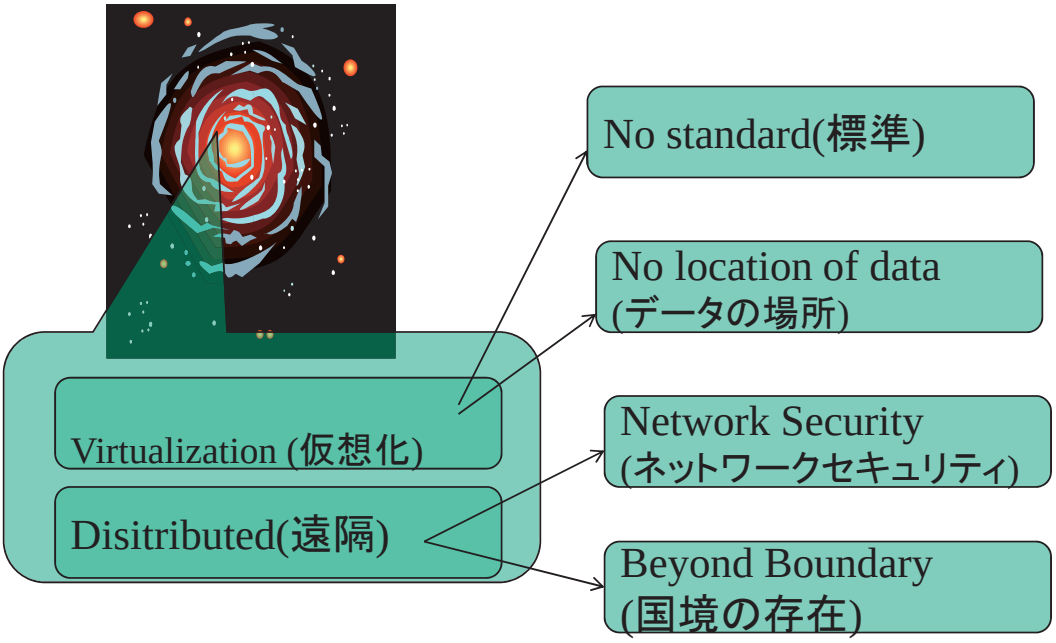
「高等教育機関におけるネットワーク運用ガイドライン」による

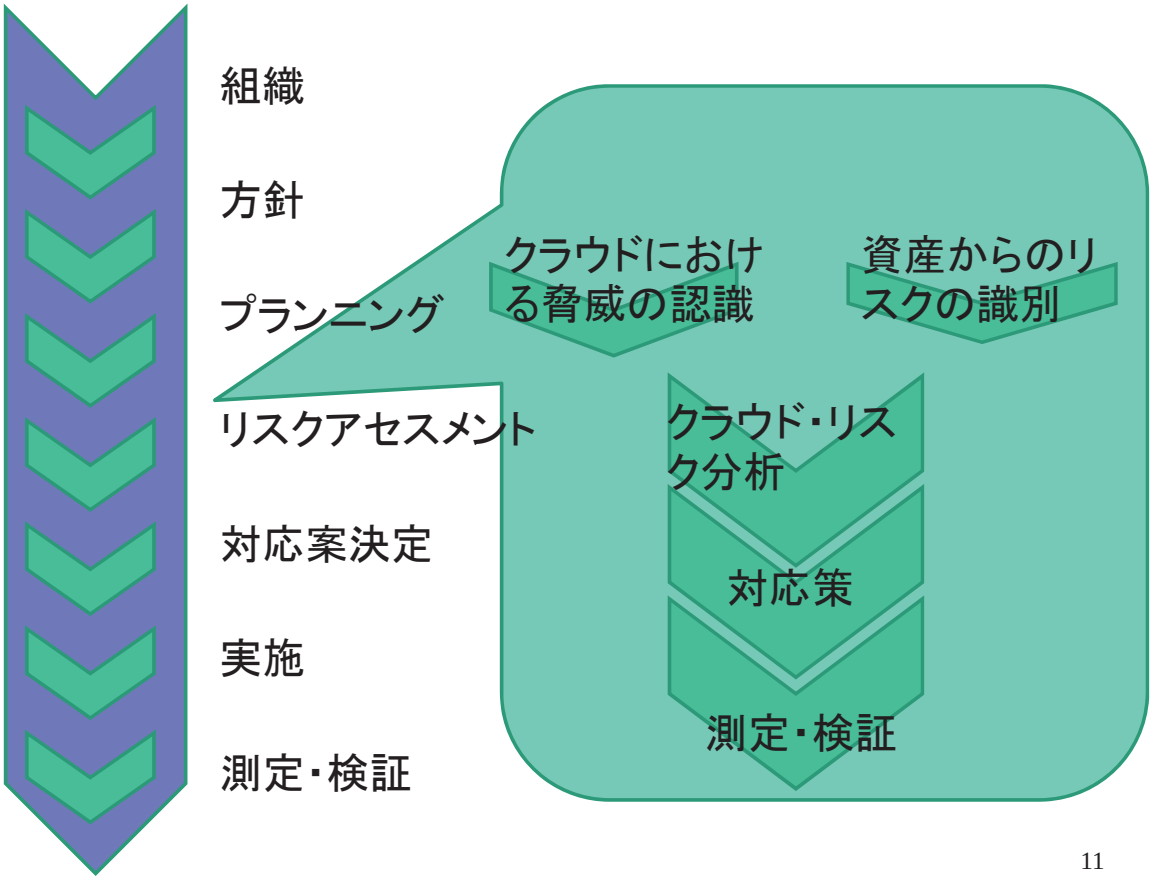
クラウドの利用について

- 「大学のクラウド活用における、検証と課題と対策」
  - (http://www.nii.ac.jp/service/openforum/forum20123/)
- アカデミッククラウドに関する研究
  - http://www.icer.kyushu-u.ac.jp/topics_ac_20140213
- 一般的な問題について
  - 日本クラウド・セキュリティアライアンス

クラウドコンピューティングの要素

“仮想化技術もしくは分散コンピュータ技術”





クラウドでの法適用の問題

- 民事上の問題についても、適用される法律を決定するのは、きわめて種々の問題が存在する。
  - ひとつの例
    - 情報主体（日本在住）のデータを処理していた利用者（日本企業）から、委託をうけていたクラウド事業者(例えば、iCloud情報流出事件(2014))
    - 脆弱性対応を怠り、流出させた
    - クラウド事業者が、外国に存在していたとする。情報主体が、クラウド事業者 に対して、プライバシー侵害を根拠に損害賠償を求めうるか
    - 日本法の考え方 対 米国での考え方

運用等に関して発生する他機関への責任問題

質問2: 学内の掲示板で、ゼミでの議論に関して、一般の人も参加しうる方針でいとなんでいるものがあります。その掲示板に名誉毀損の表現が掲載されて、被害者が、名誉毀損だとして削除を求めましたが、管理者が、名誉毀損には、あたらないとして削除をしませんでした。被害者が、この掲示板を管理している大学に対して名誉毀損だとして損害賠償請求訴訟を提起してきました。
大学は、損害賠償の責任を負うのでしょうか。

また、学内のネットワークを利用した学生が、学外の組織に対して、無権限アクセスを行って、学外の重要な情報を取得したようです。このような学生のネットワーク利用を認めていたことから大学の責任が発生するということはあるのでしょうか。

(追加)学外には、公開されていない情報(無線LAN のPSK/業務システムのアクセス方法等)を教職員・学生が、一般に公開されているところに公開することは、法律違反になるのでしょうか。

運用等に関して発生する他機関への責任問題 2

大学や研究機関などが研究会などを開いた際、主催組織の構成員でない者に対して無線LAN などでインターネットアクセスを提供した場合に、法律的な問題はあるのでしょうか。

学内に設置する携帯電話の基地局経由で違法行為が行われた場合、大学側はどこまでの法的責任を負うのでしょうか？また、当該通信事業者に対してどこまでの情報を開示を要求できるものなのでしょうか？

T大学事件

東京地判 平成11年9月24日

- 入学手続きのさいに衝突が発生した事件(自治会ないし新聞会の正当性をめぐる争い)
- 被告Aが、原告らに対して名誉を毀損する文書を大学の教養教育用のパソコンのシステム内の学生個人の利用資格に基づいて開設していたホームページ内に掲載。
- 原告らは、大学当局に抗議文書を発送した。大学当局は、リンク停止措置をとり、また情報教育担当教員は、当初、被告Aに、原告の趣旨を伝えるにとどめていた。

裁判所の判断 1

- 「被害者保護のために運営委員会に情報の削除権は認められているというよりは、T大教育研究用情報処理システムの信用を維持するというT大構成員全体の利益のために運営委員会に情報の削除権が認められているものと解される」
  - 裁判所は情報教育担当教員が原告らに対する関係において本件文書の削除義務を負うという結論を導き出すことはできない
  - 外部の者との関係について(略) ネットワークの管理者が会社との関係において被害の防止に向けた何らかの措置をとる義務が生じるかどうかは問題となった刑罰法規や私法秩序の内容によって異なる

裁判所の判断 2

- ネットワークからインターネット経由で外部にコンピューターウイルスを流す行為がなされたり、他のコンピューターに不法に侵入してシステムを破壊する行為がなされたりした場合(略) 条理上の義務として、その行為を妨げるための措置を可能な限度でとるべき義務が生じる
- 名誉棄損行為-「被害者と加害者の両名のみが利害関係を有する当事者であり、当事者以外の一般人の利益を侵害するおそれも少なく、管理者においては当該文書が名誉毀損に当たるかどうかの判断も困難なことが多い」-、「加害者でも被害者でもないネットワーク管理者に対して名誉毀損行為の被害者に被害が発生することを防止すべき私法上の義務があるわけではない」としている。

著作権等の知的侵害に対する寄与の責任

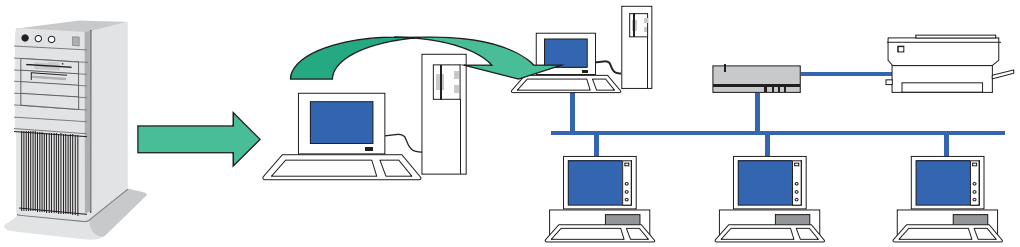
- P2Pにおける著作権侵害
  - ナップスター事件やファイルローグ事件
  - 「JASRACやBSAなど権利者7団体、全国の大学にファイル共有ソフトに関する要請文を送付(2010年ほか)」
- それを黙認している場合に大学等はどのような責任を負うか

大学等の責任

- この決定は、行為者以外の寄与者でも利益状況等によっては、当事者と同視されるという意味
- 但し、大学等においては、特別の利益を受けることはないので、この法理の射程を強く受けることはないであろう。
- プロバイダ責任制限法の定めを参考に

P2Pの提供者(ファイルローグ事件)

- ファイルローグの行為が、送信可能化、および自動公衆送信権を侵害するか否かについては、外部の者の行為の内容・性質、事業者のする送信可能化状態に対するファイルローグの管理・支配の程度、本件行為によって生ずるファイルローグの利益の状況等を総合斟酌して判断。
- ファイル情報の提供者について、直接の侵害者の侵害か第三者の侵害かの点をあまり明確にせずに、一定の要件のもとに直接侵害者と同様の責任を負わせた
- なお、平成15年12月17日東京地裁判決は、MMO側に約7000万円の支払いと差止を認めた



ユーザー

セキュリティの遵守義務違反の法的責任

- 攻撃者の利用の「踏み台」などにされ被害者に対する損害が発生した場合
  - 損害賠償の責めに任じられるのでないか
- 管理者自体が、システムのセキュリティホールに対してアップデートなどをしていない場合
  - 何らかの損害が発生する
  - 脆弱性を放置している場合に、サイト構築を請け負った業者の責任を認めた判決が出ている。
- ただし、大学自体に管理しうる状況がありえない場合は、別であろう

大学の研究員による脆弱性をついた不正アクセス事件

- 被告人(大学の研究員)
- 著作権の啓発を行う団体が運用するサイトに使われている特定のプログラムの脆弱性を発見
- 脆弱性を利用して、個人情報を引き出した。
- 渋谷のクラブで開かれたセキュリティに関するシンポジウムで手法および個人情報を公開
- 東京地裁平成17年3月25日判決-有罪

大学のコメント

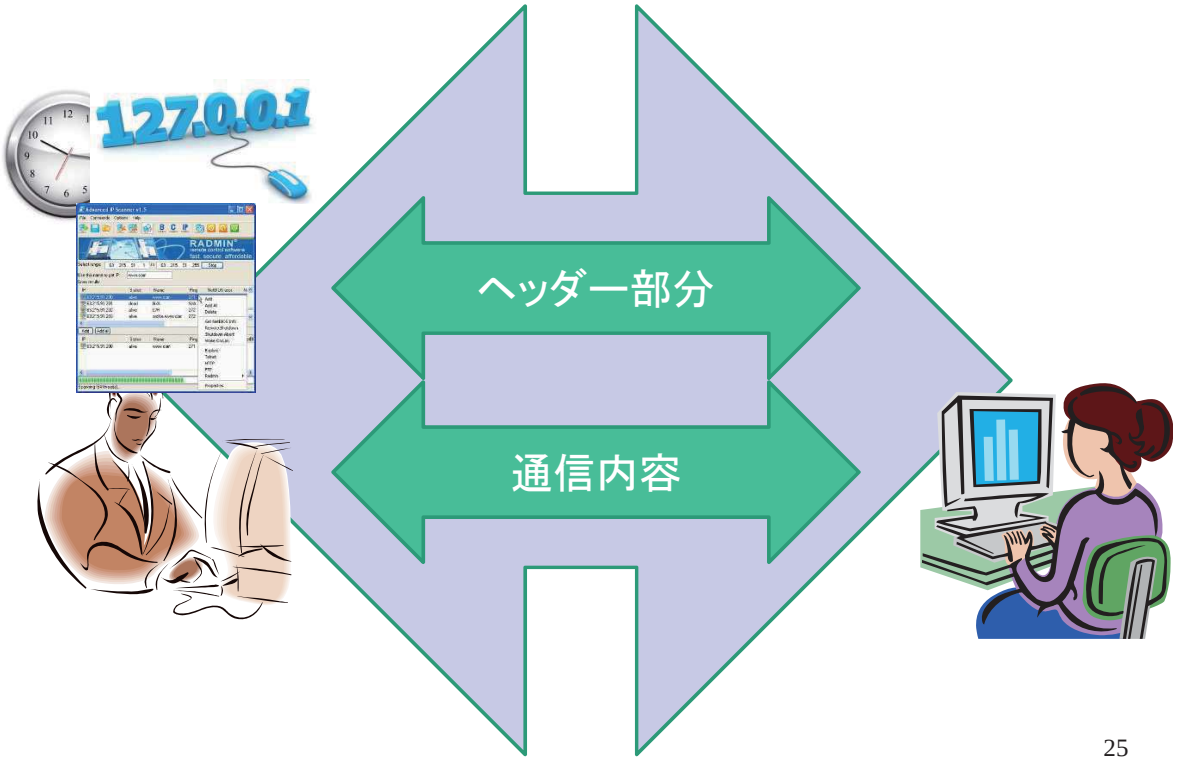
- 新聞記事
  - K大学-所属組織等の教授らが記者会見
  - 教授は「パスワードなどは盗んでおらず、不正アクセスにはあたらないとみていた。警視庁の踏み込んだ判断に驚いている。今後の司法判断を見守りたい」と困惑した表情で語った
- 検討対象
  - T2大学　全裸教員出現の非常事態収束させた危機対応力分析(http://www.news-postseven.com/archives/20150117_298226.html?PAGE=2)

ネットワーク管理と通信の秘密

- 通信の秘密について

質問3　:学内ネットワークの通信ログを運用の向上のために利用したいと考えています。この場合に、学内の利用規定に、一般的な規定として、運用向上のために利用することが記載されていますが、各利用者から個別に許諾を得る必要があるでしょうか。
また、自分の研究のために、学外から、学内のサーバに対する通信のログを分析して、近時のネットワーク攻撃の分析をしたいと考えています。通信の秘密との関係の問題はありませんでしょうか。

通信と託された情報

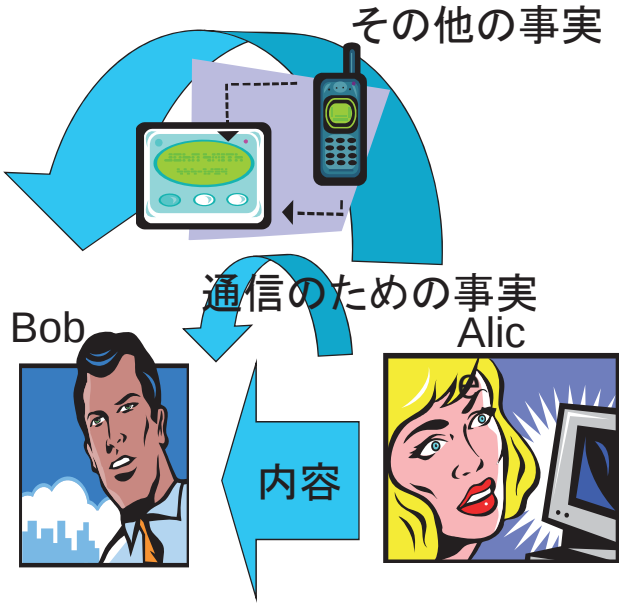


通信の秘密の現在の解釈(1)

- 電気通信事業法4条（秘密の保護）
  - 「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
  - ２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」
- 電気通信法制研究会「逐条解説　電気通信事業法」
  - 「通信の秘密を保護する趣旨は個人の私生活の自由を保護し個人生活の安寧を保証する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、憲法第21条2項の規定を受けて思想表現の自由の保障を実効あらしめることにある。そして自由闊達な通信がなされることを保証するための規定である」

通信の秘密の現在の解釈(2)

- 「通信の秘密」と「他人の秘密」(逐条解説)
  - 「通信の秘密」-通信内容にとどまらず、通信当事者の住所、氏名、発信場所と通信の構成要素や通信回数との通信の存在の事実
  - 「他人の秘密」-通信当事者の人相、言葉の訛りやプッシュホンに記憶された相手番号等直接の通信の構成要素とはいえないが、それを推知させうるものを含む



通信の秘密の現在の解釈(3)

- 電気通信事業法第4条の解釈
  - (1)積極的知得行為の禁止-通信の秘密および通信の存在自体について調査の対象とはされないこと。
  - (2)漏洩行為の禁止-通信事業者によって職務上知り得た通信に関する情報を漏洩されないこと。
  - (3)窃用の禁止ー(自己または他人の利益のために？)通信に関する情報を利用しないこと。
- 解釈の帰結(消費者行政課的見解)
  - 中間者は、正当業務行為等の違法性阻却事由がないと行動できない(ルーティング自体も「秘密」侵害の構成要件該当)
- 同意について
  - 個別・具体的な同意である必要がある(？)

「通信」の意味

- 一連の解釈における通信は、種々のデータから、「一意の通信」であることが「識別しうること」が前提
  - 識別しうることとは、結局は、コストパフォーマンスによる
- 通信の全体としての傾向としての「トラヒック・データ」については、上記秘密の対象にはならない

問題に対する回答は

- 学内ネットワークの通信ログを運用の向上のために利用したいと考えています。この場合に、学内の利用規定に、一般的な規定として、運用向上のために利用することが記載されていますが、各利用者から個別に許諾を得る必要があるでしょうか。
  - 通信ログは、個別の通信を特定しうるのか-Yes
  - 特定しえないような形に加工するのはどうか-Yes
  - 許諾は、個別・具体的であることを要するのか、どうか-微妙
- また、自分の研究のために、学外から、学内のサーバに対する通信のログを分析して、近時のネットワーク攻撃の分析をしたいと考えています。通信の秘密との関係の問題はありませんでしょうか。
  - 通信の秘密の例外規定の解釈-不明
  - 個人情報保護の例外規定が参考に

近時の大学のネットワーク構築の法律問題

- 大学のサービスの一般化と電気通信事業法

質問4：私の大学では、こんど、学内の無線LAN AP にケータイキャリアのワイヤレス・アクセスポイントサービスを相乗りさせて、毎月の利用料をもらうこととなったのですが、大学自体が、電気通信事業者としての届出をしなければならないのでしょうか。
そもそも、電気通信事業者の届出をしないとどのような問題がおきるのでしょうか。
無線アクセスサービスを学内ネットワークへの入り口として利用する場合には、なにか異なるのでしょうか。

クリッカー　2

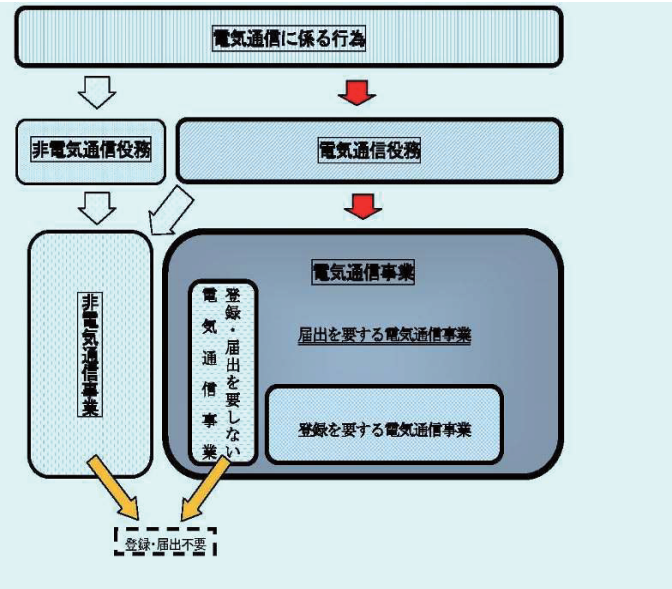
- 大学のネットワーク接続設備であっても「電気通信事業者になりうる可能性があること」について
- １　よく知っている
- ２　だいたい知っている
- ３　名前だけは知っている
- ４　知らない

電気通信事業とは？/ 登録･届出？

- 電気通信事業法1条
  - 「電気通信事業の公共性」にかんがみ、
  - 「その運営を適正かつ合理的なものとするとともに、その公正な競争を促進することにより、電気通信役務の円滑な提供を確保するとともにその利用者の利益を保護」
- 同法9条
  - 電気通信事業を営もうとする者は、総務大臣の登録を受けなければならない。
  - ただし、総務省令で定める基準を超えない場合-届出

電気通信事業とは？営むとは？

- 「電気通信事業参入マニュアル［追補版］」
  - 届出等の要否に関する考え方及び事例―
  - (http://www.soumu.go.jp/main_content/000267716.pdf)



電気通信役務

- 「電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供するもの」
  - 他人の通信
    - 自己間の通信以外の通信をいい、他人と他人との間の通信のほか、自己と他人との間の通信も含む。
- 電気通信設備を他人の通信の用に供する場合に合致しない場合
  - 「電気通信」に関して
    - 場所貸し
    - 携帯電話の代理店
  - 「他人の通信」に関して
    - 企業における内線電話、LAN
    - 自社データベースアクセスサービス

電気通信事業者

- 「電気通信役務」を「他人の需要に応ずる」ために提供する「事業」
  - 登録/届出/それらが不要
  - 「他人の需要に応ずるため」
    - 自己の需要に応じているものは含まれない。
      - Webサイト開設・通販対応
  - 「事業」(反復・継続)
    - 非常災害発生対応等は含まれない
    - ホテル電話・ホテルインターネット
      - 宿泊サービスに付随して電話の設置・運営を行っており、電気通信役務の提供が独立した事業として把握できないことから、電気通信事業に該当しない。

電気通信事業を「営む」

- 「営む」
  - その対価として料金を徴収することにより電気通信事業自体で利益を上げようとすること、すなわち、収益事業を行う場合をいう
  - 料金を徴収していないとしても、実質的に電気通信役務の提供により利益を上げているとみなされるときには、「電気通信事業を営む」に該当する

回答は？

- 学内の無線LAN AP にケータイキャリアのワイヤレス・アクセスポイントサービスを相乗り
  - 場所貸しといえますか？
  - アクセスが大学の事業として利益をもたらすもののように設計されている可能性はありますか？

日本クラウド・セキュリティアライアンスご紹介

- 2010年に法人格なき社団として結成
- 2013年に法人化
- LinkedInやFacebook等で情報交換しています。
- アカデミッククラウドの問題を検討するのでしたら、是非ともご参加いただき、Wg等を提案いただければ、前向きに対応できるかと思います。

法律問題のご相談・ネットワーク関係の調査は

- 2F駒澤綜合法律事務所
- 4 株式会社ITリサーチ・アート
- ikuo@comit.jp