大学のセキュリティ
～ITガバナンスの視点から～

京都大学学術情報メディアセンター
上原哲太郎
uehara@media.kyoto-u.ac.jp
http://uehara.tetsutaro.jp/

大学における情報セキュリティの位置づけ

- ネット社会の一員としての責務
  - ウィルスや踏み台で「よそに迷惑をかけない」
    - インターネットを育てたのは大学だが、
      インターネットを無法地帯にしたのも大学かも？
- 大学の「ブランド」を守るため
- 社会からの要請に応えるため
  - 高まる情報セキュリティ/プライバシーに関する意識
  - 「研究してくれ」「教育してから社会に出してくれ」
- 政府からの要請に応えるため
  - 情報セキュリティ基本計画
  - 「知的財産立国」
- 個人情報保護法などへのコンプライアンス
- 訴訟リスクへの対応

大学の情報セキュリティ上の脅威

- 外部からの脅威
  - ネット越しのハッキング／ウィルス（bot）
  - 部外者による不正利用（踏み台・公開端末・無線LAN）
  - 物理的盗難→情報漏えいの危険
- 内部の脅威
  - 構成員によるネットの不正利用
    （アタック・掲示板荒らし・P2P・・・）
  - 情報持ち出し・漏えい（今のところあまり顕在化してない）
- 番外
  - 構成員による不祥事（Blog、SNS、一般事件…）
    - 乗じて「アタック」が…
  - 著作権法違反

何故こんなことになっているのか

- 歴史的問題が圧倒的に大きい
  - 「実験」の名残り・・・タダで使い放題　サーバ立て放題
  - 学生・ボランティアによる管理体制のツケ
    - 特に研究側にはまじめな管理体制が未だに不在
- システム管理は誰にでも出来るという幻想
  - 「動く」と「管理する」の差は大きいのに・・・
  - 一度動かしてしまうと既得権益が発生→自縄自縛
- 学生という「扱いにくい存在」
  - 教育する前に既に「悪い使い方」に慣れてる
  - 何をするにも「100％」は無理

「電算センターでナントカしてくれ」

- ネットワーク構成の見直し
  - クライアント系のローカルIPへの閉じ込め
- アンチウィルスソフトウェアの導入
  - クライアントに全部入れるのが徹底できない・・・
  - メールサーバが無数にあって・・・
- ファイアウォールの導入
  - 設定のコンセンサスは？
- IDSの導入
  - とにかく監視し続けるのが大変
    - 何かわかったときにアクションを起こすのはもっと大変
  - 監視＝検閲という反応が多い

研究できない！

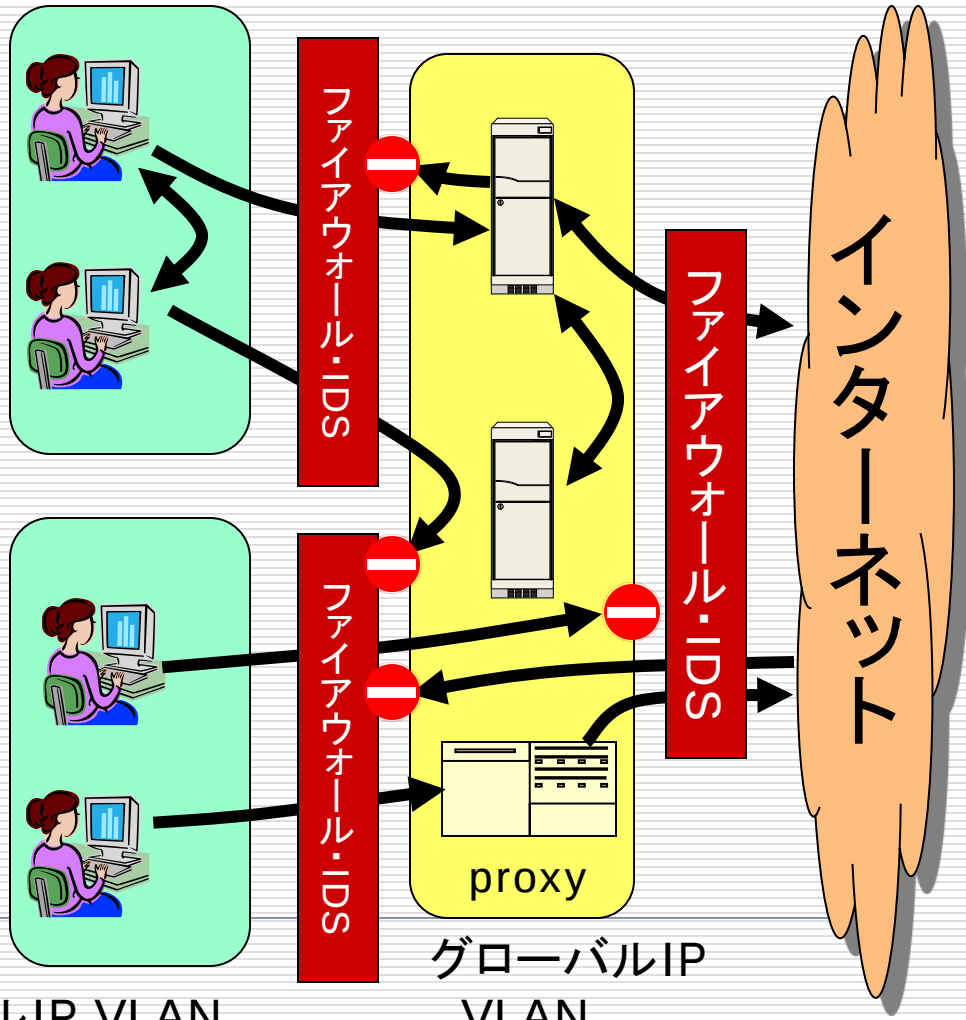
重いから代えて

なぜこのポートを…

学問の自由！

京大キャンパスLANの論理的構成

- 単一のグローバルIP空間と、多数のローカルIP空間からなる
  - グローバルIPは完全登録制・固定IPのみ・課金あり
  - ローカルIPはDHCPが基本
  - ローカルIPはさらに2種類の設定（オープンスペース／クローズドスペース）
- グローバルIP空間とインターネットの間はほぼ素通し
  - 希望によりポート毎の設定可能
- ローカルIPからグローバルIPへは出られるが逆はダメ
- ローカルIPとインターネット間は通信不能
- ローカルIP VLAN間の通信も原則不許可
- IDSによる常時監視
- ウィルスチェックの一元化（SPAM対策がエサ）



「とにかくインシデントを封じよう」

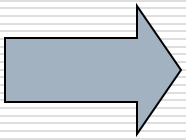
- 京大でまず頑張ったのはインシデント対応
  - 外部からの通報またはIDS監視結果で
    不正アクセスやbot感染等を見つけたら
    ネットワーク危機管理委員会に報告、
    決定後直ちにCISOの権限で
    ネットワークから当該機器を遮断する
  - ネットワーク遮断された機器は、当該部局から
    部局長名で報告書が提出され対応がなされた
    ことが確認できないと解除できない

ここまでやっても残る問題

- インシデントは大きくは減らない
- 攻撃の高度化により
  インシデント自体が「見えない化」してる不安
  - ウィルスも不正アクセスも
- 「末端のインシデント・レスポンス」が不備
  - 再発防止策は部局任せにするしかないが
    その能力が十分にあるとは限らない
- 人的問題への対応が大変「重い」
  - 不祥事、誹謗中傷、ハラスメント…

技術だけではどうしようもない

- 技術で対処療法してても限界はすぐくる
- 人的問題対応にはユーザ教育が必要だが…
  - 全員講習の難しさ　e-Learningの強制力の限界
- 情報セキュリティポリシーを作ってはいるが
  マネジメントが機能しているか？？



ガバナンスの欠如が根本的問題

情報セキュリティマネジメントとは

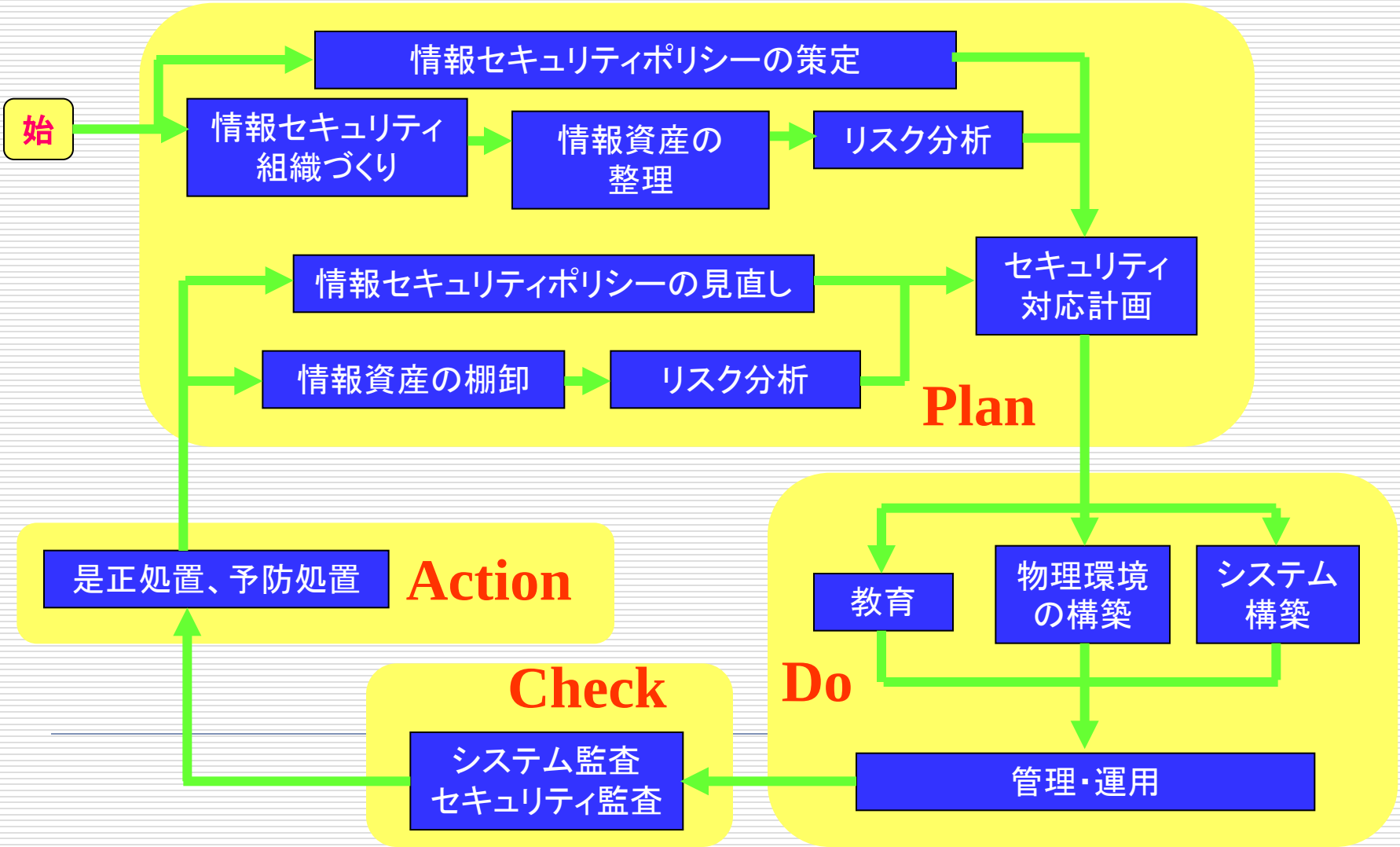
- 情報資産について次の事柄を「維持」すること
  - Confidentiality（機密性)
    - 情報をアクセス権に従い管理する
  - Integrity(完全性）
    - 情報の内容を正確に保つ
  - Availability(可用性）
    - 必要なときに常に利用できるように運用する
- これを実現するのが情報セキュリティマネジメントシステム（ISMS)
- BS7799、ISO27001、JIS X 5080等で規格化
  - 実はISO9001/ISO14001などと似た流れ
  - 認定制度としてJIPDECのISMS認証制度など

いわゆる
「情報のCIA」

情報セキュリティポリシーとは

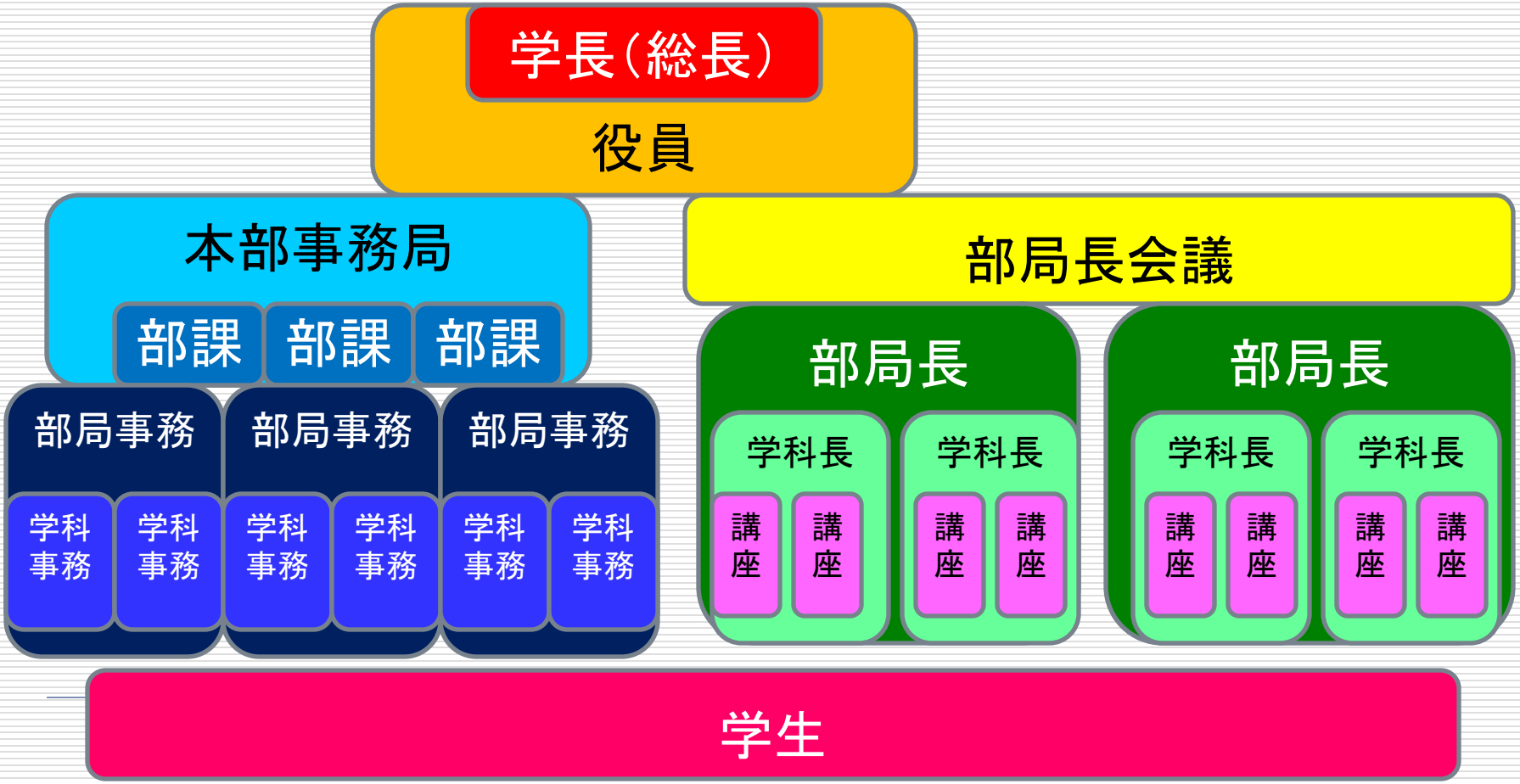
- 情報セキュリティマネジメントシステムを維持するための方針や具体的基準・手順をまとめたもの
- 3段階の文書からなる
  - 基本方針（ポリシー：組織で1つ）
    - 組織の情報資産をどのような脅威からどのようにして守るかについての基本的な考え方
  - 対策基準（スタンダード：組織または部門単位）
    - 基本方針を実現するために何をやらなければならないかという遵守すべき行為及び判断などの基準
  - 実施手順（プロシジャ：各担当向け）
    - 対策基準に基づいた、業務、情報システムまたは職務ごとの具体的なセキュリティ対策の手順書、マニュアル等
- これらの文書を段階的に策定し構成員に守らせる

セキュリティポリシーのPDCAサイクル



大学の組織的問題点
＝はっきりしない指揮系統

- 国立大学の場合…



マネジメント上の「カベ」

- 部局の自治、教員の自主独立
  - 特に教員は組織帰属意識が…
- 部局事務への指揮系統混乱
  - 本部事務と部局長による二重統治
- 事務の「縦割り体質」＋ITアレルギー
  - 予算システムとの問題（ボトムアップ調達）
  - ITが絡むとセンター任せor業者任せ
- 学生はそもそもマネジメント枠外
  - 私物パソコン持ち込みを制限は困難
  - 留学生は「前提が置けない」

そもそも組織運営がボトムアップ的

しかし、ついに尻に火がついた

- 大学全入時代の到来
  - 運営効率改善は喫緊の課題
- 国公立に来た「前代未聞の予算削減圧力」
  - 特に国立大学は中期財政フレームの影響
    人権費外の予算はここ3年で2～3割
    削減しないとあわない
  - ITは削減対象として狙われやすい
    - そもそも額が大きくて目立つ
    - レンタル契約上、一度契約すると5年前後継続的な支出が発生する→今後の変動に耐えられるか
    - 特にセキュリティは「不要不急」扱いされがち

いよいよトップダウンで決断しなきゃいけない事態に

しかしトップダウンといっても…

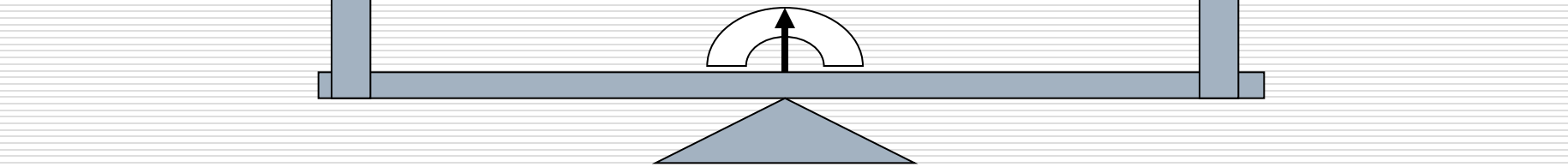
求められるのは
結果ばかりで
プロセスに対して
ケアしてもらえない
失敗の責任は
しっかり負わされる
これで組織と
言えるのか？！

トップに求められること

業務効率化

利便性向上

安全性確保



バランス確保のために
トップの判断が不可欠

IT使った業務効率改善って…

- 「定型業務の一括集中処理」「中抜き」「外注」
  - 本質的に同一の業務は同一システムにする
    - 部局毎にルールが違うとカスタマイズ費用大
  - 事務的中間チェックを機械化することによって段数を減らす
- その前提となるのは…
  - 業務のテンプレート化　←「歴史的経緯・部局の特殊事情」をどこまでガマンできるか？
  - 技術的には「認証を中心とした管理の一元化」

京都大学で進んでいること
(あまり自慢できませんが)

- 統合認証システムの構築運用
- 教職員ポータル・学生ポータルの構築
- 電子メールの管理一元化
  - 教職員向け全学メールシステムの運用開始
  - 学生向けシステムとの統合（12月中）
- 教務システムの統一展開（KULASIS）
- 職員向けグループウェアの一元運用
- 学内で「クラウド型ホスティング」をサービス

集中管理とセキュリティ

- 集中管理はセキュリティを向上させると言われる
  - 「サーバモンキー」からサーバを剥ぎ適切な管理
  - システム全般に同一のポリシー適用しやすい
- その一方で…
  - アプリケーションセキュリティは本当に向上するか？
    - 特に研究向けは目が届かない
    - 業務関係はパッケージ頼りだが…
  - 可用性が失われたときのインパクトが大きいのでその対策にコストがかかるが…
  - 認証が統合されているがために破られると終わりかといって認証方式を強固にすると…
    - 複数の認証方式を提供？

集中管理は特効薬ではない

今後必要になってくること

- そもそも大学にとって本当のITリスクは？
  - 教員にとって身近な分だけ/目立つだけに
    これまで「研究向けITシステム」のセキュリティが
    良く話題になってきたが…
  - 本質的なリスクは事務系、特に教務系に

- 効率的IT投資とセキュリティ確保のために
  役員の近くに「ITと業務とセキュリティに強い」
  人材を確保するべきではないか

こういうことができる人
（CIO補佐、CSIO補佐）

専門家の仕事

現状のシステムの
XXが問題です

対策しないと
何が起きるのかね

XXという脅威が
XX程度あります

コンプライアンスとの
関係は？

XX法への対応上
問題になります

業務への
影響は？

メリットは・・
デメリットは・・・

対策案と
コストは？

システム変更と
業務フローの見直しで・・・

コミュニケーションが重要

高すぎる！時間も
かかる！別案は？

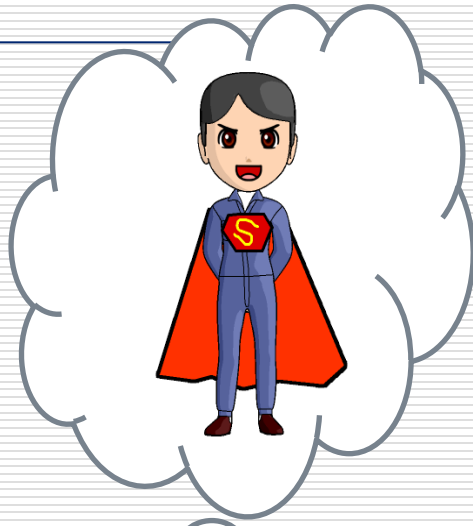
高度IT技術者に求められるもの

- ITによる業務効率化を牽引できる知識
  - 適切なソリューションを導入・展開
    - ジレンマ：ITによる効率化の本質は「中抜き」
人的チェック機能の低下は内部不正の呼び水
- 安定運用可能なシステムがデザインできる能力
  - 適切な設計・十分なテスト・運用への「見極め」
  - トラブル対応＝BCP(事業継続計画)の策定運用
    - ジレンマ：どこまでアウトソーシング？
- セキュリティへの対応
  - 事故防止、情報漏洩防止技術を適切に導入
  - インシデント発生時はBCPに沿って・・・
    - ジレンマ：業務効率化とのバランス

広く・深く・バランスよく

さらに望めるなら…

- セキュリティインシデント対応力への要求
  - 技術では防ぎきれない内部不正への対応
  - 個人情報漏洩時の「社会的責任への対応」
  - 刑事事件発生時のフォレンジック対応
- コンプライアンスへの対応
  - 個人情報保護法、プロバイダ責任制限法・・・
    - 法がシステムのデザインにも関わる
  - セキュリティ/プライバシポリシーの展開
    - 業務効率への影響を最小化することが必要
  - 業務システムとIT統制・内部不正防止との関係
  - 訴訟発生時のe-Discovery対応



覚えることが多すぎる　技術バカでは対応できない

そんな人がいるの？？

- むしろ「育てる」のが必要なのでは？？
  - 内部に「最高級の教員」がこんなに揃ってるはずなのにどうしてこれまで内部で人材育成できなかった？？？
- 急には無理なので外部からの雇用？

- いずれにせよ人事設計から手を入れないと
- 広義のIT投資として一時的に重点化しないと

おわりに

- 大学はガバナンス確保がこれまで難しかった
  - そもそも全てがボトムアップで動いていた
  - 学生はまた別のルールで動いている
- しかし現状は本当に危機的状態
  - 予算圧力は大変厳しい

- IT投資にガバナンスを、メリハリを
- それを支える人材の確保を