

# 大学におけるクラウド活用

～仮想集約化から学内クラウドと将来像～

関東学院大学 情報科学センター  
小糸 達夫

2013年1月28日



1



## 関東学院大学の概要



創立：1884年  
(大学設置：1949年)



学生数：約12,000名



5学部、4研究科、法科大学院



キリスト教を建学の精神にもつ  
総合大学



2013年4月より、理工学部、建築・環境学部、  
看護学部が開設



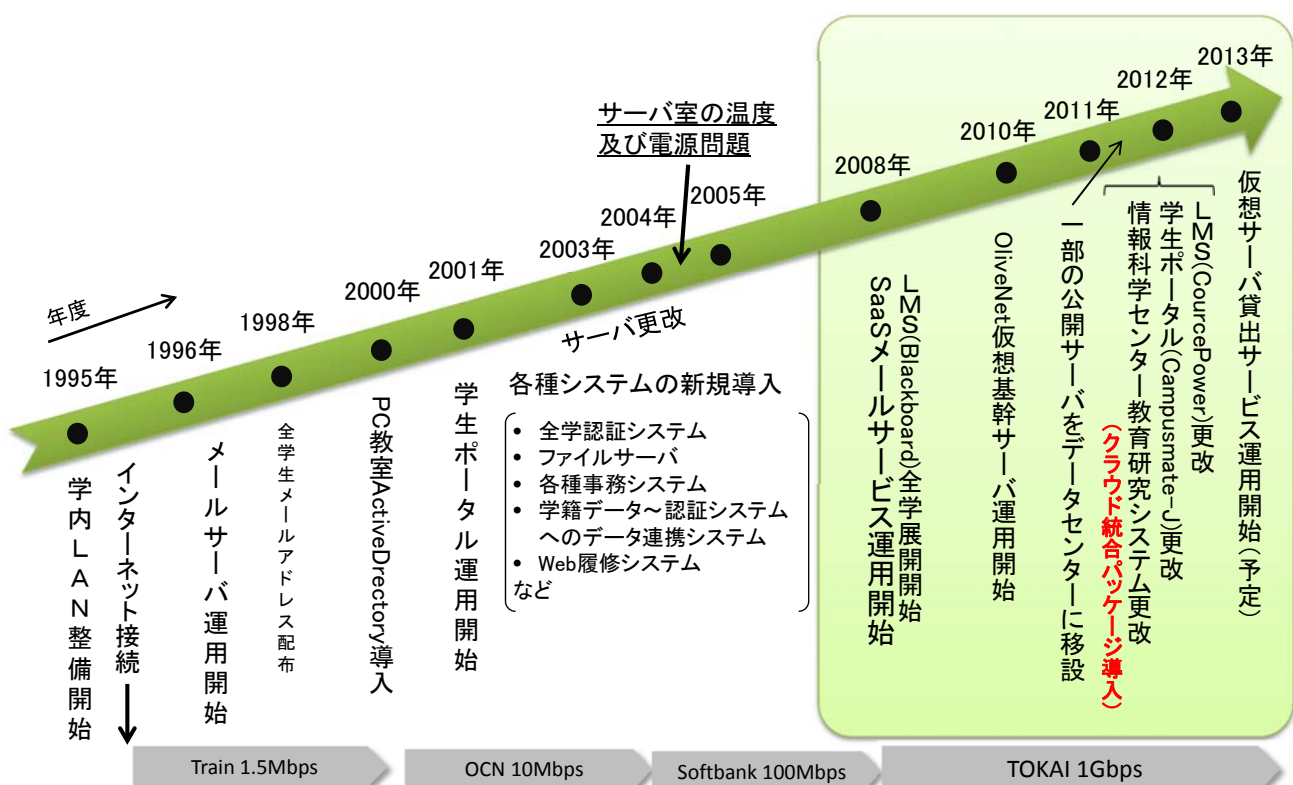
2



## 本日の内容「大学におけるクラウド活用」

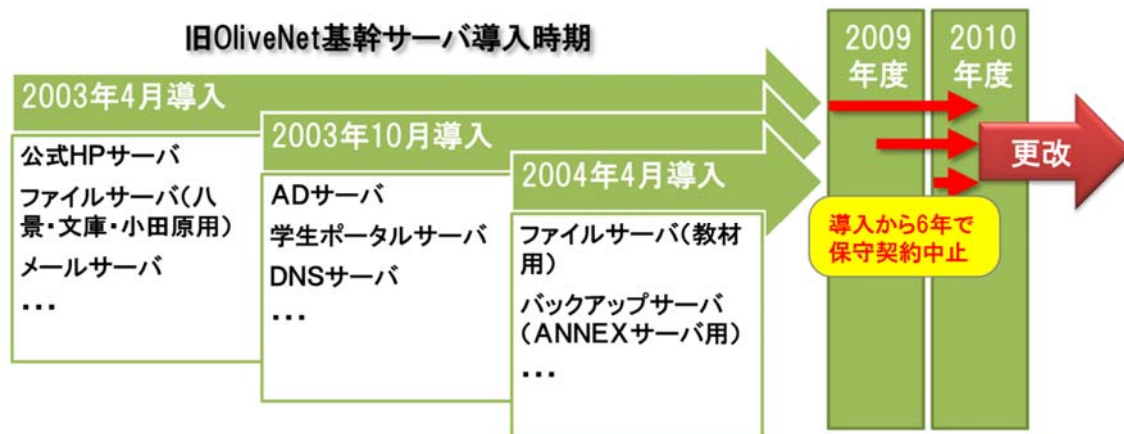
- **経緯**
  - － 本学の情報化への取り組み
  - － 従来システムの問題点
- **メールシステムのクラウドサービスへの移行**
- **仮想集約化の取り組みについて**
  - － 物理サーバ満載の悪夢からの脱却
- **震災後の事業継続対応**
  - － 一部のサーバをデータセンターへ移設
  - － WAN・インターネット回線の見直し
- **教員向け仮想リソースの貸出サービスの展開**
  - － 経緯～実施方法……問題点、課題
- **今後の学内クラウドの方向性について**
  - － これまでの取り組みの最適化と新たな技術の取り込み

## 経緯： 本学の情報化への取り組み



## 経緯： 従来システムの問題点

- 必要に応じてサーバを追加してきたため、サーバの導入時期がバラバラ。
- サーバ台数の増加の影響でサーバ室の電気容量不足・空調能力の限界  
⇒ 空調は18度設定、しかし夏は室温28度を超える。
- 設置スペースの不足
- 冗長構成を考慮していないことから、保守作業時のサービス停止が避けられない。
- 年数経過によりハードウェア保守契約が締結できない時期を迎える。



7

## 【2008年4月】メールシステムのクラウドサービスへの移行

目的： サービス停止による利用者への影響が大きいメールシステムを基幹サーバの更改前に事前に安定稼働できるようなシステムを見直しておく。

### SaaSメールサービス選定のポイント

- メールシステムの安定稼働が実現可能なこと。
- Webメールの機能を有していること
- 問い合わせなどのサポート体制が充実していること。  
⇒ 無償メールサービスはサポート体制に不安残る。
- 稼働中の統合認証システムの認証連携が利用できること。  
⇒ GoogleApps、Live@Mailは認証連携の条件が合わない。



### 商用のSaaSメールサービス(ネットマークス株)を選定

- 本学の認証連携システムに合わせたサービス提供が受けられた。
- 既に契約していたネットワーク運用管理体制(常駐による業務委託)を使ったサポート体制で対応できた。

8

## 【2008年4月】メールシステムのクラウドサービスへの移行

### メールサービス仕様

- OfficePlanetメールサービス (Zimbra) ネットマークス(株)
- メールボックス 1人あたり1GB
- Webメール、POP、IMAP、迷惑メールフィルタ



### 移行後の状況

- インターネット経由の利用となったが、レスポンス不足は無かった。
- 迷惑メールの認識率が飛躍的に向上した。
- セキュリティ対策や運用管理から解放された。  
⇒ 脆弱性対策や定期保守作業(深夜に実施)は全てお任せ。

### 問題点

- メールボックス容量が少ない。(経費面でこれ以上増やせない)
- コスト高である。  
24時間365日安心安全なシステム運用、セキュリティ対策や運用管理面から解放されることは管理者側にとってはメリットが大きいですが……。
- システムトラブルがあった際は復旧するのを待つしかない。何もできない。
- Zimbraをターゲットにしたパスワード奪取のSpamメール被害が増加傾向。

## 【2010年10月】仮想集約化の取り組み

### 条件1

- 多数のサーバを仮想化により集約して物理サーバの台数を減らし、稼働率の向上を図る。
- サーバ室の許容電力、空調能力にあったサーバに更改する。

### 仮想化基盤の導入

- DMZ/イントラゾーンに仮想化基盤を導入し、仮想サーバ上に各サービスを構築して、サーバの集約・稼働率向上を実現する。

### 条件2

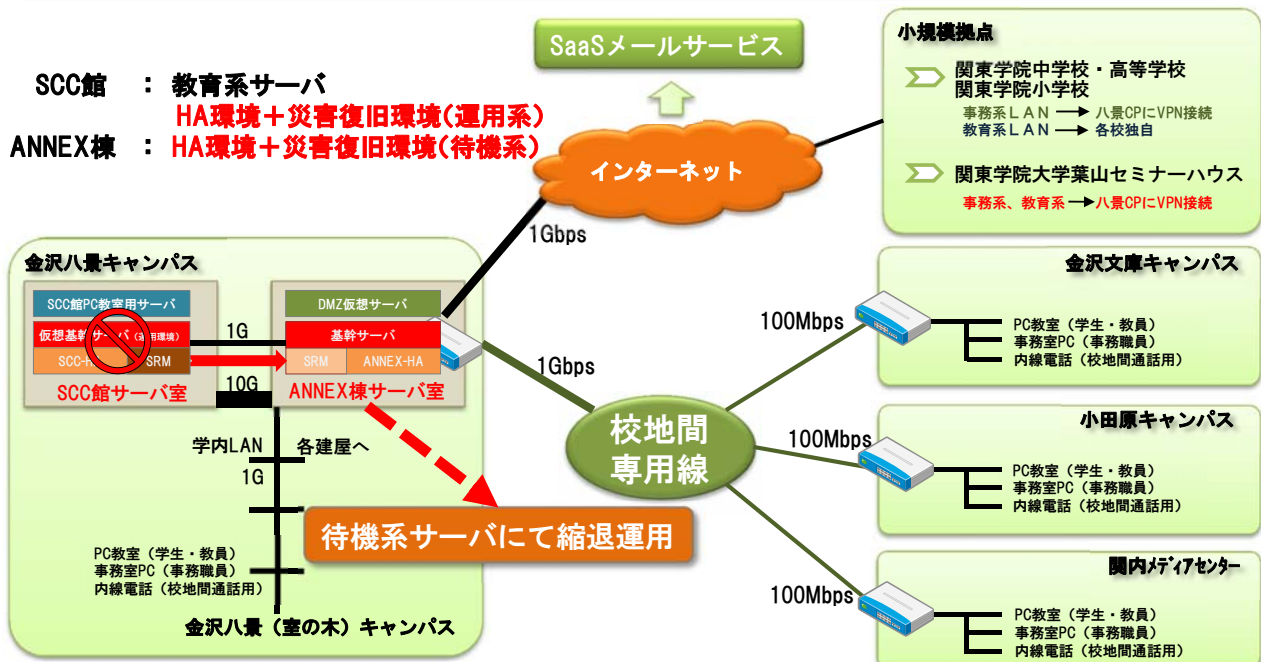
- 2つの建屋にあるサーバ室を有効活用し、サービスの継続的な運用を実現できるようにする。
- システムのメンテナンスや建屋のメンテナンス(停電等)時にサービス停止を極力少なくするような構成とする。
- 災害復旧に対応したシステム構成とする。

### 災害対策/利用サービスの継続のための基盤システムの構築

- ストレージ(仮想領域とユーザデータ領域)を集約し、2つのサーバ室間でデータのレプリケーションを行い、二重化を行う。
- 災害時におけるシステム復旧を実現するため、信頼性と管理性に優れた迅速かつ低コストな災害復旧の仕組み(待機系は縮退運転設計)を実現する。



## 【2010年10月】仮想集約化の取り組み



災害復旧時は、最低限の学生サービスが提供できるサーバに限定し、ANNEX棟待機環境で運用を継続させることが可能。

前提条件: SCC館又はANNEX棟のいずれかが停電

## 【2011年12月末】震災後の事業継続対応

### 東日本大震災当日の状況

- 情報設備のシステム自体には被害なし
- 金沢文庫キャンパスを含め周辺地域が翌日まで停電
- OliveNet仮想基幹サーバ等は免震架台により影響なし
- システムは問題なく稼働していた

### 震災以降の対応

- 大学臨時休校の周知  
⇒ 公式HP、学生ポータル、LMSを活用したお知らせ発信
- 安否確認 ⇒ Eメールを活用
- 計画停電対応 ⇒ 仮想基幹サーバの手動停止及び起動作業

↓  
問題点

1. 仮想基幹サーバの停止・起動には1~2時間を要する。
2. システムの停止中は公式HP等が利用できない。
3. システムの停止中は他キャンパスの情報システムは利用ができない。

## 【2011年12月末】震災後の事業継続対応

### 3・11以降の新たな課題

- 災害時や計画停電等を見据え、仮想基幹サーバの構成の再検討が必要  
⇒ 事業継続を何処まで考えるのか？
- 災害時に必要なサービス  
⇒ 学生や教職員への周知のためのシステムは災害時でも稼働させたい。  
⇒ 学内PC(事務、PC教室)でインターネット利用は最低限必要。  
⇒ 金沢八景キャンパスが停電になっても他キャンパスのネットワークは利用できるようにしたい。(インターネットやメール)

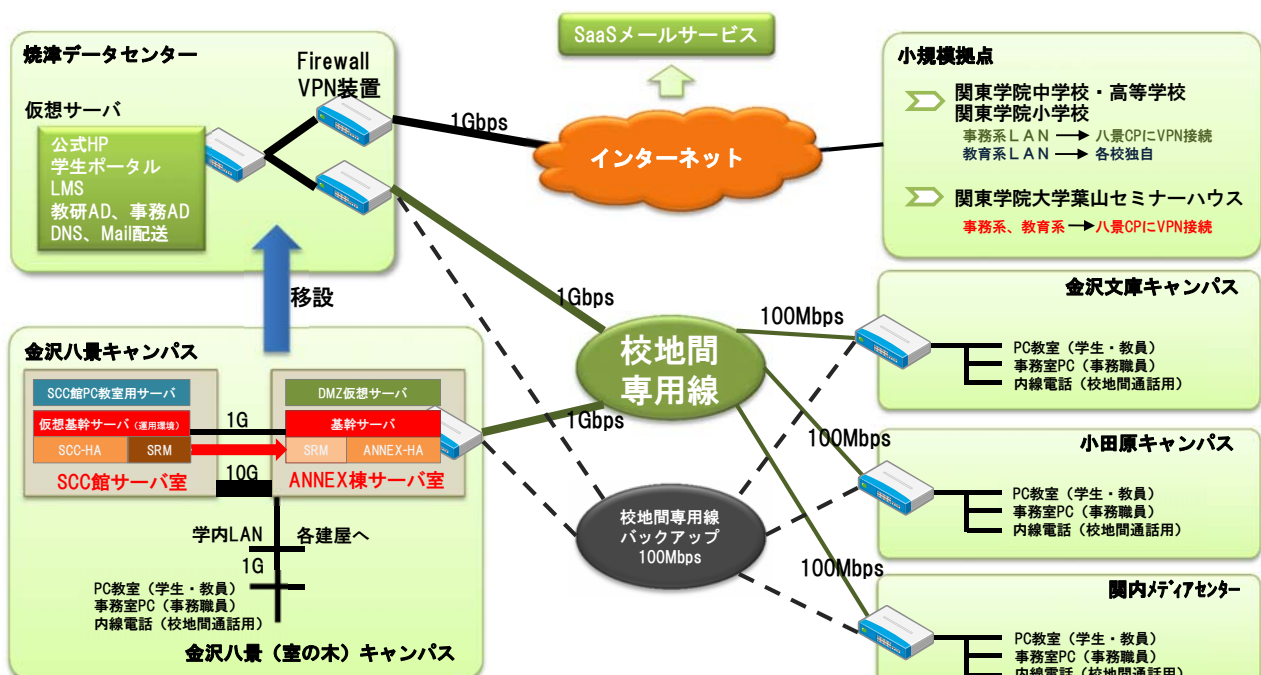


## データセンターを活用する

1. 公式HP、学生ポータル、LMS等の公開サーバをデータセンターに設置する。
2. インターネット回線を金沢八景キャンパスからデータセンターに移設する。
3. データセンターを校地間専用線の接続拠点とする。

## 【2011年12月末】震災後の事業継続対応

- ① 金沢八景キャンパスのネットワーク中心拠点機能をデータセンターに移設。
- ② 公式HPや公開サーバをデータセンターで稼働させ災害時の継続稼働を目指す。



## 教員向け仮想リソースの貸出サービスの展開

### (1) 経緯

- 情報科学センターの教育研究用システム更改(2012年4月運用開始)
- 教員からの要望  
⇒「センター管理のサーバを使って、公開用のサーバを構築したい」



## 仮想サーバの貸出サービス(課金制)の展開 (2013年4月サービス開始予定)



### 実現方法

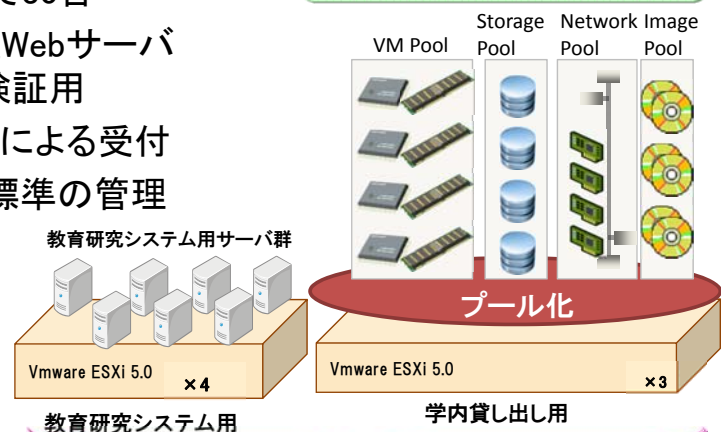
- センターの教育研究用システムの運用に必要なサーバを仮想集約化した際の空きリソースを貸出用としてクラスタ分けすることで対応
- 課金のためのログ管理や将来的な自動貸出サービス展開を視野に入れるため、プライベートクラウド統合パッケージを導入。  
⇒導入作業工数や導入コストの削減にも貢献

## 教員向け仮想リソースの貸出サービスの展開

### (2) 全体構成

- 3台の仮想サーバを貸出用に割当て
- 想定最大ゲストOS: 最少構成で30台
- 主な用途: moodle、研究用途Webサーバ  
各種システムの検証用
- サービス開始時点では申請書による受付
- 電源投入切断は、パッケージ標準の管理Web画面を利用。  
(コンソール操作ができない。)
- サーバへのアクセスは、RDP(Windows)、VNC(Linux)
- 課金制度  
月額利用料を研究費等で負担。

仮想サーバ要件  
 雛形OS : Windows Server 2008 R2  
 Red Hat Enterprise Linux 6 (64bit)  
 ハード : メモリ×4GB、CPU×1つ、HDD:60GBのサーバ×30台を想定

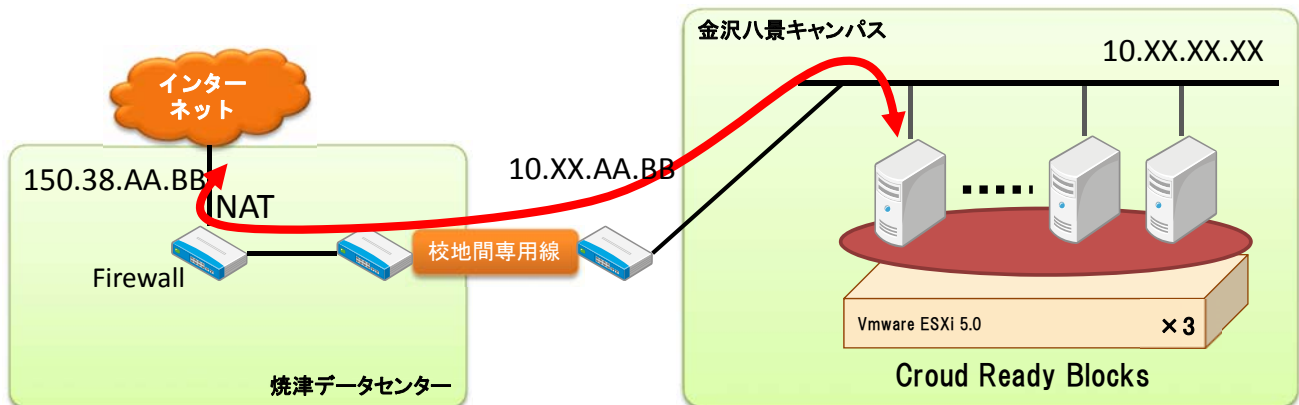




## 教員向け仮想リソースの貸出サービスの展開

### (3) ネットワーク構成

- ゲストOSは、プライベートアドレスで割り当て(学内ポリシー)
- 学外からのアクセスは、データセンターのFirewallでNAT(1対1)
- DNSは公開用(グローバルアドレス)、内部用(プライベートアドレス)に設定。  
⇒ 学内端末は内部用DNSを参照するようになっている



センターで管理できない仮想サーバに外部からのアクセスを許可するためには、何らかのセキュリティ対策や監視が必要。

17

## 教員向け仮想リソースの貸出サービスの展開

### (4) 問題点

- パッケージ製品であることから希望しているようなカスタマイズができない。
- あくまでも企業向け製品。教育機関向けには使いにくい。  
⇒ 開発側の考えと大学側ニーズ(思い)に相違  
⇒ 電源操作はWebGUI。コンソール接続機能は無く、RDP又はVNCを別途用意。
- Linuxが商用製品(RedHat)しか対応していない。(CentOSは利用不可)
- 貸出用サーバだけでシステムを導入すると、経費負担は割高である。  
⇒ 他の基幹システムとの共存という方策で無ければ費用対効果は悪い。
- ネットワークのセキュリティ対策には課題が残る。  
⇒ Firewallを入れたいがボトルネック  
⇒ 教員の管理するサーバを何処まで監視するのか？

18

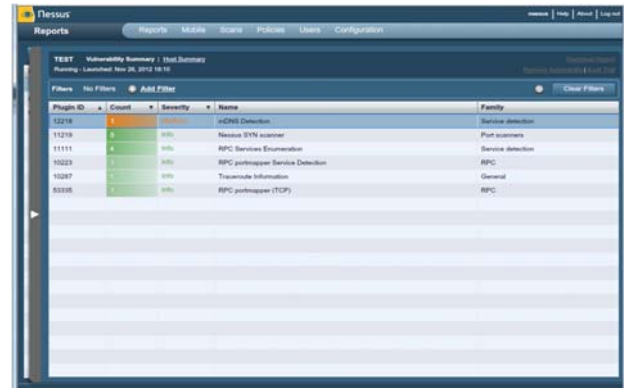
## 教員向け仮想リソースの貸出サービスの展開

### (5) サーバの脆弱性監視

- 管理者(教員)にiptables等で利用するポート以外は遮断するよう指導する。
- 学外からのアクセスを希望するサーバの場合、解放ポートの申請を受け、サーバの構築が完了した時点で Nessusを利用して脆弱性チェックを行う。  
⇒問題なければFirewallのルール設定を行う。
- 定期的にNessusで対象サーバの脆弱性チェックを行う。



スキャンポリシー画面



レポート詳細情報

## 今後の学内クラウドの方向性について

### これまでの学内クラウドの取り組みから得た教訓

- **災害対策環境は設計段階で有効性を慎重に判断すべき**
  - ⇒ 構成が複雑であるため、自前で運用が難しい。
  - ⇒ SiteRecoveryは時間がかかる。授業運営面では最適とは言えない。
  - ⇒ 止めたくないサーバはデータセンターへの移行を第一に検討。
  - ⇒ 冗長化、二重化は目的を明確にする。
- **学内クラウドを構築するなら構成はできるだけ簡単に！**
  - ⇒ 今までの環境や構成をそのまま集約すると収集がつかない。
  - ⇒ 大規模集約はシステム起動、停止に時間がかかる場合がある。
- **停電に関する想定は十分に考慮して設計を行うこと**
  - ⇒ ストレージ関係の起動・停止時間はよく確認すること。
  - ⇒ UPSの保持時間内に正常停止ができるか？
  - ⇒ 復帰後の手動操作は必要となるのか？

## 今後の学内クラウドの方向性について

### 本学が次期システムで目指すこと

従来 ⇒ インフラ整備だけの視点  
今後 ⇒ 組織的な取り組みの下でのインフラ整備

#### (1) 情報管理の明確化

- ・ データの持ち出しのための対策(セキュリティ面や管理面)
- ・ 大量の蓄積データ(ログ)の管理

└─→ PC利用状況ログ、LMS利用ログ、etc

#### (2) 災害時の事業継続、データ保全対策の再検討

- ・ データセンター(クラウドサービス)の積極的な活用
- ・ 業務端末のシンクライアント化
- ・ 学内クラウドとクラウドサービスの使い分け