# 大学における情報管理のあり方と暗号学的視点からの文書の長期保存について


奈良先端科学技術大学院大学
猪俣敦夫

Nara Institute of Science and Technology NAIST ®

# 自己紹介

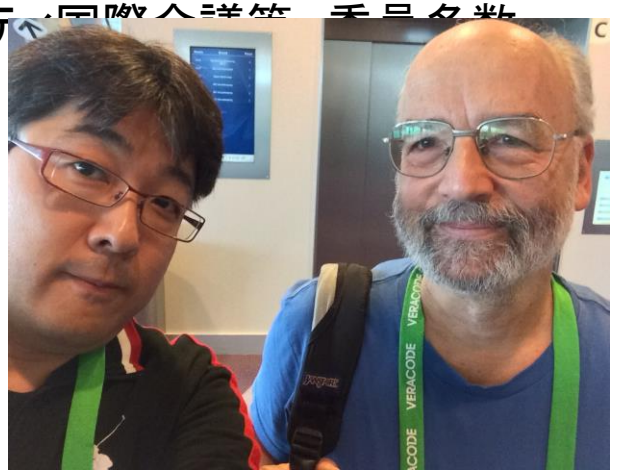
- 1973年、この世に生まれる
- 1976年、D-H鍵共有が生み出される
- 1978年、Rivest, Shamir, AdlemanによってRSAが産声をあげる
- 1994年、RSA-192が破られる(IFP分解）
- 2002年、RSA解読にはまる、楕円曲線暗号にもはまり高速実装にひたすら取り組む
- 2008年、教育と研究(現実逃避)の傍ら、情報セキュリティ人材育成に取り組む

- 奈良先端科学技術大学院大学　准教授
  - 京都女子大学、奈良女子大学、慶應義塾大学、同志社大学　非常勤講師
  - ベネッセHD　情報セキュリティ監視委員、情報セキュリティ国際会議等　委員多数

暗号化: $C = P^E \mod N$

復号: $P = C^D \mod N$

$P$: 平文, $C$: 暗号文,
$E$ , $N$: 公開鍵, $D$: 秘密鍵



Shamir先生@Amsterdam

大切なこと

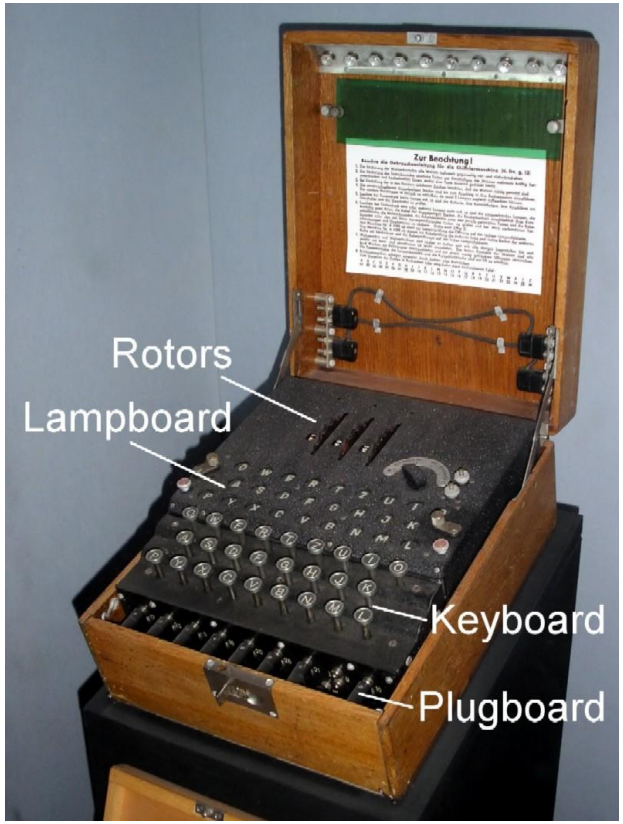
暗号化（の計算）は簡単だけど、復号（の計算）はとてもとても難しい

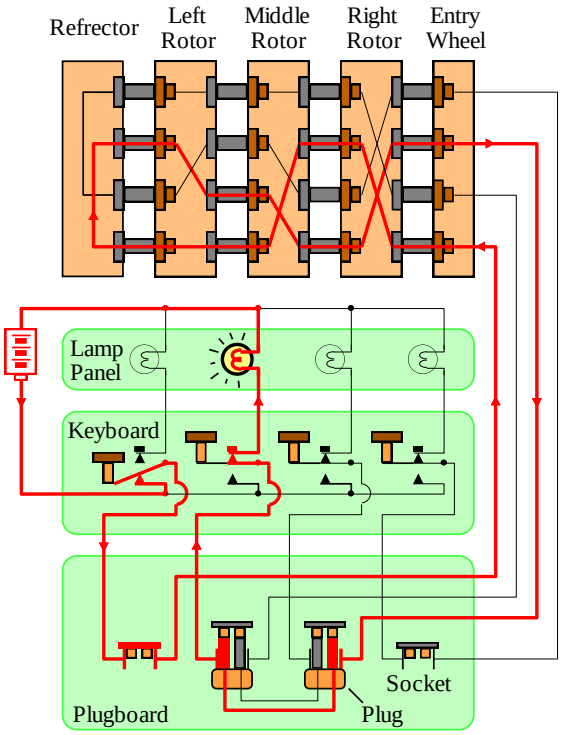
# 本日の話題

1. 暗号の強さとは何であるかを考えてみる
2. 企業と大学の情報管理の大きな違いについて、大学システムの一例を俯瞰した上でリスクを整理してみる
   - 忘れ去られた冷蔵庫の奥底には何が?
   - 内部犯行(ミス)もなく自由に活動できる場を実現できるのか?
3. 暗号学の視点からみた電子文書(データ)の長期保存を考えてみる

# Enigma

- 第2次世界大戦でドイツ軍が使用していた最強の暗号機
  - A-Z(26個)ポジションを持つローターによってランダムに変換が行われる換字式暗号
    - キー入力の度にローターが回転して変換規則が変化
  - ローター（スクランブラ）の種類と位置が最も重要な秘密鍵




暗号機の構造や暗号文自体が解読に重要な統計情報を含んでいる



http://mm.ahs.kitasato-u.ac.jp/~lm00000/sim/ueyama_ip/history/enigma.htm

# 辻井重男先生所有の実機

## エニグマ

### スクランブラー

キーボードで押されたアルファベットを変換する「鍵」。このエニグマは10個ついている。
（ドイツ軍が使用していたのは3個～5個）

押すたびにそれぞれの歯車がランダムに動く

### ランプボード

電球が内蔵されている。
キーボードを押すと、スクランブラーに対応するアルファベットが点灯する

### キーボード

平文・または暗号文を入力する

### 取り付けランプボード

取り出して茶色のケーブルで本体と接続すると（写真下）、ランプボードと同じアルファベットが点灯する

キーボードは重いので、キーボードを打つ人と、ランプに表示されたアルファベットを記録する人に分担し、スムーズに作業できるような配慮にしたと思われる

### 電源

電源は、コンセントかバッテリーを選ぶことができ、電圧も調節可能だ

中央大学研究開発機構の資料より

# 「法」という素晴らしき世界

- A mod C とは?
  - AをCで割った余り
    - 27 mod 12 = ?
    - 39 mod 12 = ?
  - Cを法とする世界
    - 12を法（mod 12)とする世界とは


- 準備 $N=p \times q$ (p, qは大きな大きな素数)のとき
- $M^d \bmod N = M$
  - $d=(p-1)(q-1)x+1$ （any $x$)
  - フェルマーの定理から証明は簡単


©kickstarterjfan

# 公開鍵暗号RSAレシピ

- 公開鍵e、秘密鍵dのつくりかた
  - $e \times d \bmod (p-1)(q-1)=1$となるようなeとd
  - 数学をうまく巧みに使いこなせたら・・・
- 暗号化　$M^{e} \longrightarrow C=M^{e} \bmod N$
- 復号　$C^{d}=M^{ed} \longrightarrow M^{ed} \longrightarrow M \bmod N$

大切なこと(しつこい・・・)

暗号化(の計算)は簡単だけど、復号(の計算)はとてもとても難しい

# 暗号は一方向性が鍵

- 暗号化は計算が簡単
  - 暗号化が難しかったらそんな暗号は誰も使わない
- 復号は計算がとてもとても難しい
  - 秘密鍵dを知らなければ普通に計算は解けない

- RSAを攻撃するということは秘密鍵dの値を（公開されている情報だけから）見つけ出すこと
  - 合成数N(=P × Q)をばらせたら可能性は見えてくる?

# 1977年当時の問題

- 合成数N=p x qの素因数分解問題
  - 1977年　RSAが紹介された記事：
    - Nが10進数で129桁＝RSA-129

公開鍵 N, e
N =114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
e =9007

暗号文 C
C =106698614368578024442868771328920154780709906633937862801226224496631063125911774470873340168597462306553968544513277109053606095

[公開鍵：N, e　暗号文C=(平文 $M^e$) mod N　秘密鍵：d]

- RSA攻撃：暗号文Cから平文Mを導出、すなわち(暗号文$^d$)を導きだせるか?
- Rivestは1977年に125桁を因数分解するには4京(40,000兆)年かかると…
  - が、1994年に1600台の計算機を用いて129桁のFactoring成功(´・ω・`)

# RSAへの攻撃（衝撃の事実）

- 画期的な解読アルゴリズムの発見・創出
  - RSA Factoring Challenge
    - 2003年12月3日　RSA-576bit
    - 2005年11月2日　RSA-640bit
      - Factoring Challengeは2007年で終了
    - 2009年12月12日　RSA-768bit
    - 201x年y月z日　RSA-1024bit　もうすぐ!?
  - Lenstraらによる数体ふるい法とその算出式
    - 現状の計算機を想定した暗号解読時間の見積もり
- 計算機環境の変化
  - CPU性能向上
  - 分散コンピューティング技術の発展
  - 量子計算機の出現

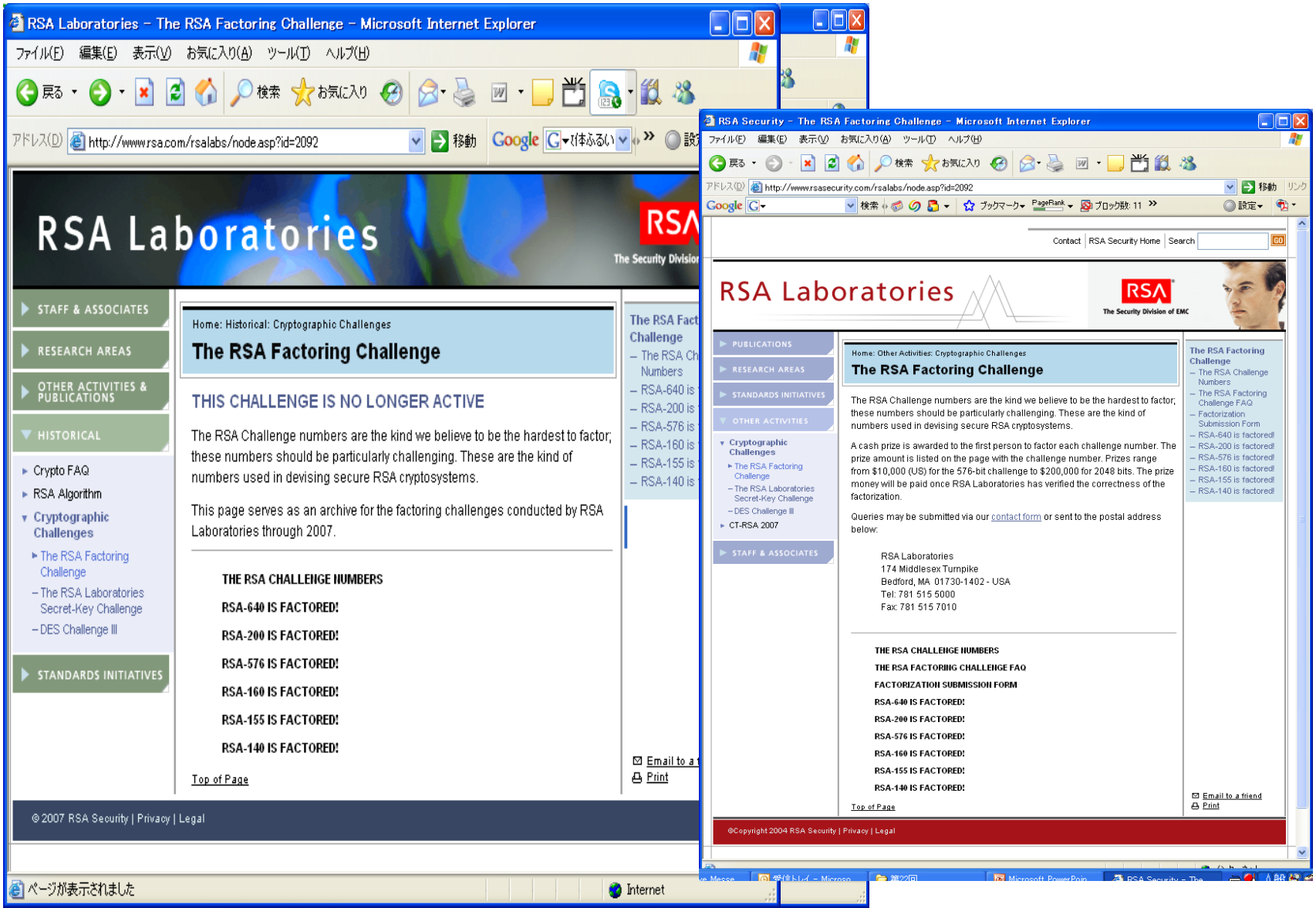
# 素因数分解問題(IFP)
# 難易度評価法

1. 現在存在しているハードウェア上でプログラムを実装し、評価を行う→RSA Challenge Contest(一般数体ふるい法:GNFSプログラム)
2. 現在の技術で作成可能だが実際には作られていないハードウェアを用いて思考実験を行う→専用H/W（FPGA/カスタムchip）
3. 現在の技術では実現不可能なハードウェアを用いて思考実験を行う→量子計算機

# 一般数体ふるい法(GNFS)実装方針

1. 多項式選択
   - 分解対象Nに対してZ上既約なf(M)≡0 (mod N)を満たすような整数係数既約多項式f(X)と整数Mを選択
2. ふるい処理
   - ふるい処理は、処理量の半分以上を占める(理論的評価、および経験則より)が、多くの処理は独立に計算可能であるため並列化効果は大
3. Filtering
   - 線形代数処理の高速化
4. 線形代数
   - Filteringから得られた行列から関係式の導出を行うため、処理の独立性が低い。このため並列化にする場合には計算機の密結合が必要
5. 平方根
   - $x^2 \equiv y^2 \pmod N$のx, yの導出を行う

# お金が目的ではない
# ただひたすら数学だけの戦い



# LenstraとVerheulによる分析

- Lenstra, A. K., E. R. Verheul“, Selecting Cryptographic Key Sizes,” *Journal of Cryptology,* Vol.14, No.4, pp.255-293, Springer-Verlag, 2001.

1. **「安全性の基準」**: DESが何年の時点で安全であるか
2. **「単位コストあたりの計算量」**: ある一定のコストでどれだけの計算速度のコンピュータを取得できるか
3. **「解読にかける予算」**: 解読にかける予算がどれだけ増加していくか
4. **「解読アルゴリズムの進化」**: 解読アルゴリズムの進化によって見積もられる計算量が減少していくか

$$L_N[s,c] = \exp((c + o(1))(\log N)^s (\log\log N)^{1-s})$$

$$L_N[1/3, (64/9)^{1/3}]$$

# 私もRSAと戦い続けてきました

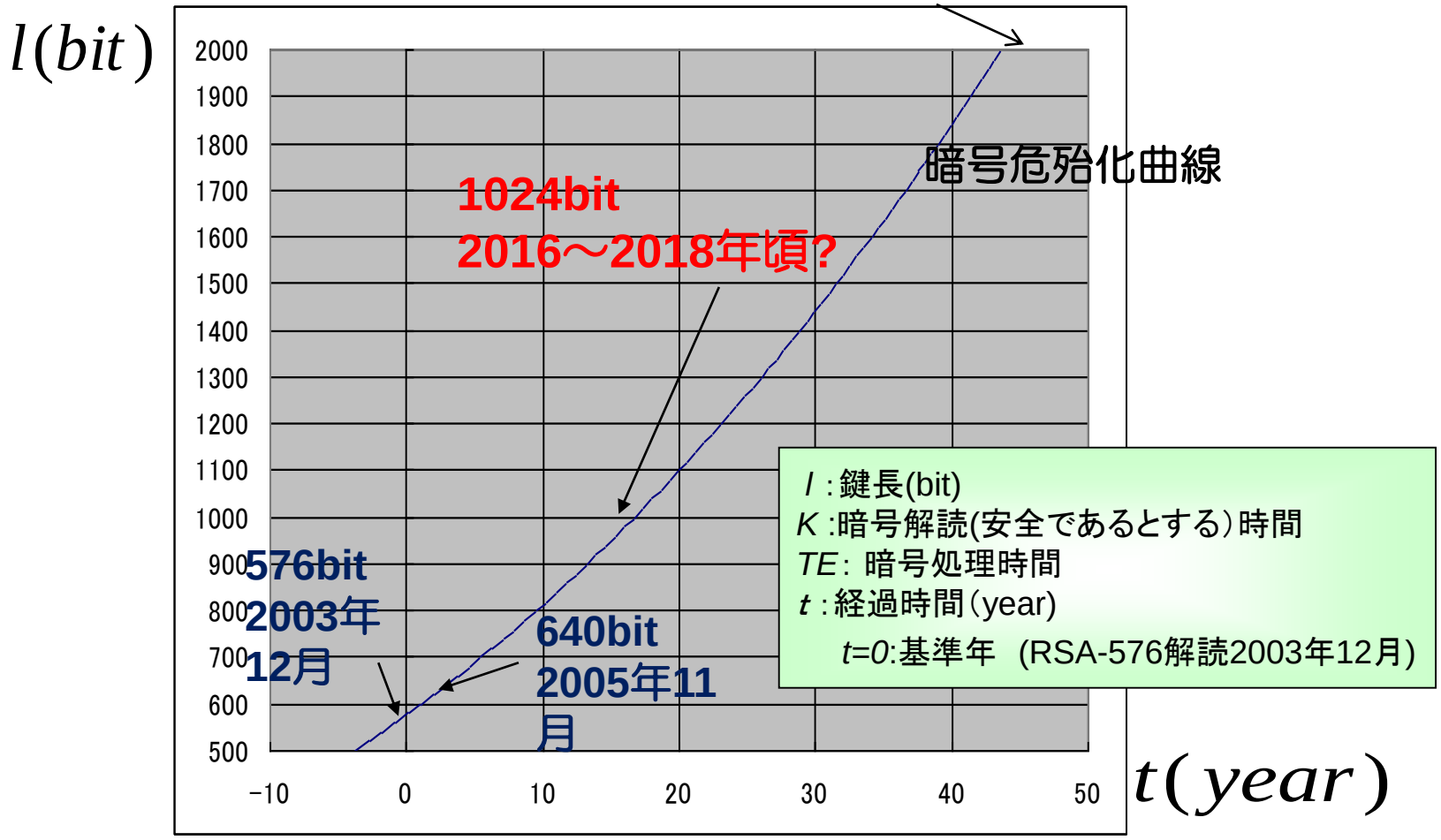
- 気づくと年ばかり重ねていく現実・・・。ここはやはり解読できた妄想をしよう
  - RSA解読計算量：一般数体ふるい法GNFS
  - 計算機速度の向上：ムーアの法則

$$t = \frac{3}{2\log 2}\left( l^{\frac{1}{3}} \log^{\frac{2}{3}} l - \log(aK) \right) + t_0$$

- $t$: 時間(年)
- $l$: 鍵のビット長(bit)
- $t_0$: 基準年
- $a$: $t=t_0$における計算速度
- $K$: 暗号解読にかかる時間

# 猪俣による妄想
# （もちろん真面目に計算しています）

では2048bitに伸張すれば?



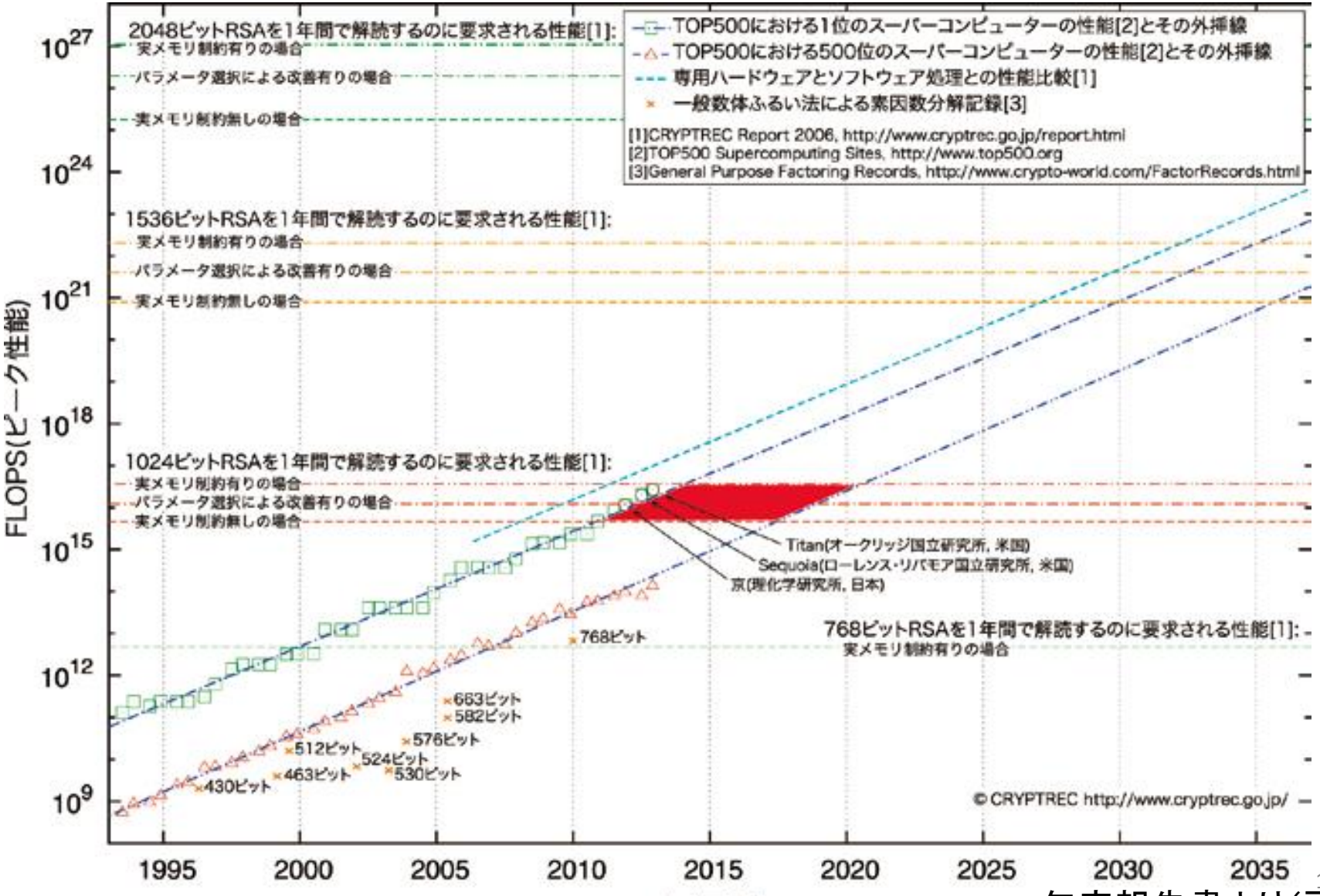

RSA暗号の安全を確保するために必要なビット長の予測

# Silvermanらによる検討

- Silverman, R. D. , “A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths,” *RSA Laboratories Bulletin, No.13, April 2000*
- 10,000,000$=1,020,000,000円のコストをかけるならば?(PentiumIII 500MHzのPC)

| 公開鍵のサイズ | 分解時間 | 計算機の台数 | メモリ容量 |
|---|---|---|---|
| 430 | 5分以内 | 100,000 | 256MB程度 |
| 760 | 50年 | 4300 | 4GB |
| 1020 | 300万年 | 114 | 170GB |
| 1620 | 10^16年 | 0.16 | 120TB |

# スパコンTOP500による
# RSA解読性能見積もり(N=p×q型IFP)




CRYPTREC　2011年度報告書より(更新版)

# 安全な鍵長サイズ
# 私たちが悩む必要があるのか

- 厳密に悩む必要は無い、が、しかし証明書発行事業者や研究者は大いに悩むべし
  - NIST、CRYPTRECの指針をしっかり確認
- 鍵長サイズを伸張することは簡単
  - しかし、世の中の動向や影響を検討し、その必要性や意義を考える必要

| 安全性等価な鍵長サイズ | 80bit | 112bit | 128bit | 192bit | 256bit |
|---|---|---|---|---|---|
| 共通鍵暗号 | 80 | 112 | 128 | 192 | 256 |
| 素因数分解 | 1024 | 2048 | 3072 | 7680 | 15360 |
| 離散対数 | 1024 | 2048 | 3072 | 7680 | 15360 |
| 楕円曲線上の離散対数 | 160 | 224 | 256 | 384 | 512 |
| ハッシュ関数 | 160 | 224 | 256 | 384 | 512 |

# 100%安全な暗号は?
# そんなものありません

- 鍵長サイズを大きくすれば当然強度は(猛烈に)増す
  - 新しい暗号アルゴリズムに置き換えるよりも・・・
  - 100円の価値しかない情報に10億円かけて守る意味は?
    - たかが100円と割り切っていいのかどうか
- どうして新しい暗号に置き換わらないの?
  - 暗号研究者としての苦節苦悩の15年・・・
  - 何とかして楕円曲線暗号(ECC)に進みたい
    - 幸か不幸かBitcoinのおかげでECDSAが日の目をみつつある
    - 短い署名長での安全性→ICチップやIoTデバイスなどメモリ制約の場
  - しかし、今時メモリの数百～数Kbitごときで悩むことなのか。単に伸張すれば良いじゃない・・・(泣)
- そして大学で保管している情報・データは長～い長～い時間守ってあげる必要がある、さてどうすれば

# 暗号の悩ましいところを見ていただいたところで少し話を変え（頭に残しておいて下さい）、本学における情報管理の取り組みを紹介します

外部非公開情報があるため、Twitter等での情報発信はご遠慮ください

m(_ _)m

# 奈良先端科学技術大学院大学

- 学部を持たない国立大学
  - 情報科学研究科
  - バイオサイエンス研究科
  - 物質創成科学研究科
- 規模
  - 教職員 355、学生 1100
  - 1991年10月創立
- 非常にコンパクト
  - 教員がやりたいことが（怒られない程度で）好きなことができる
  - まさに大学界のエストニア（笑）

# NAIST組織




# 総合情報基盤センター
# (ITC: Information iniTiative Center)

- 2010年7月設立
  - 情報科学センターと学術情報課(図書館)の統合
- 組織構成
  - 次世代システム研究グループ　　4名
  - 情報基盤技術サービスグループ　　8名
  - 学術情報サービスグループ　　14名

# NAIST曼陀羅

- 安定したサービスの提供と新しい研究基盤の実現
- Open System
  - 標準 (Internet, FS, VM, …)
- 利用者の好み
  - Unix, Windows, Macintosh

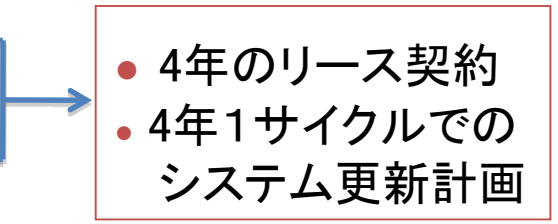
曼陀羅

（曼荼羅ではありません）

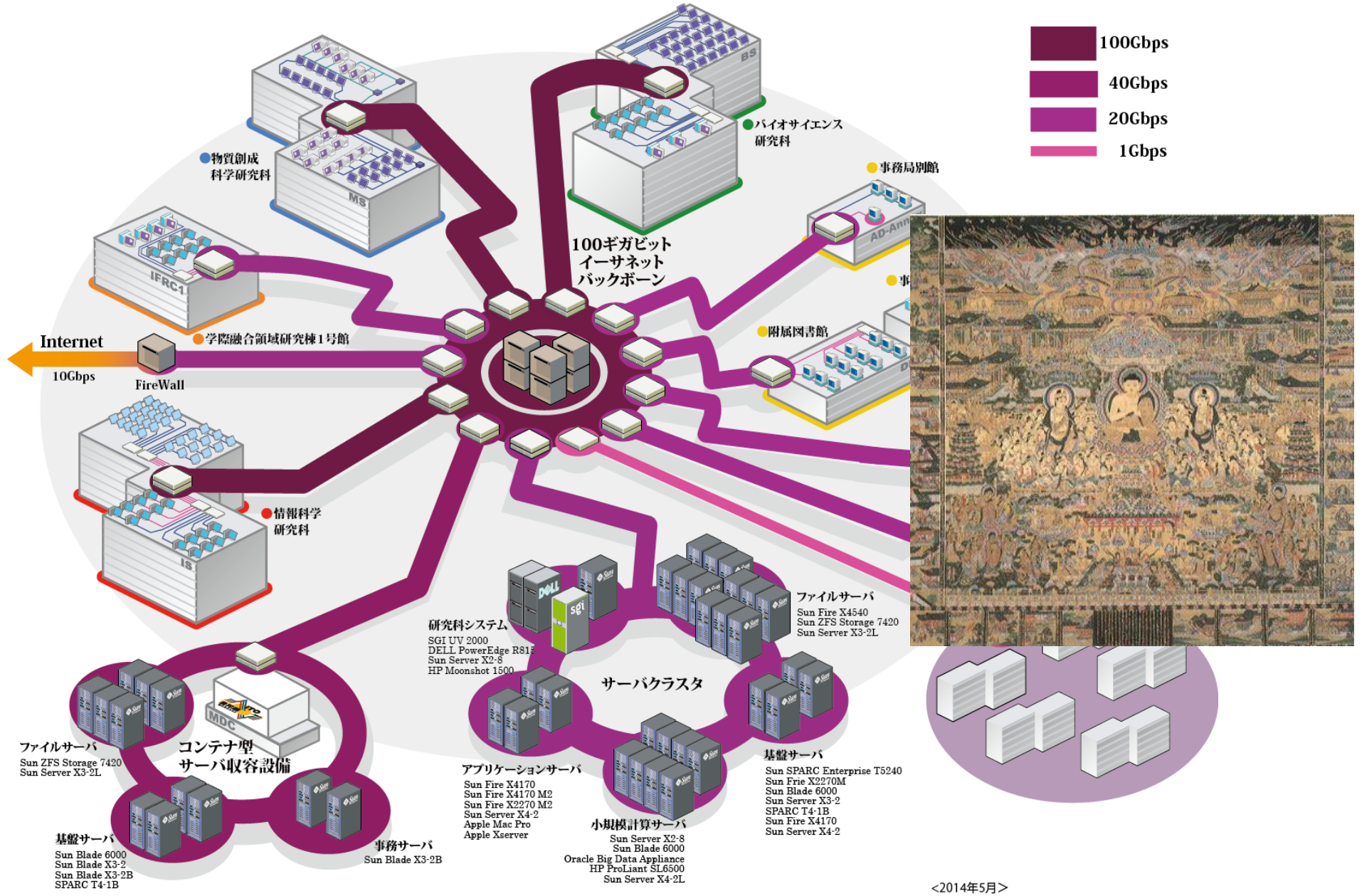
當麻寺　曼荼羅

# NAIST曼陀羅

- NAIST曼陀羅(MANDARA)
  - 最先端の研究プラットフォーム
  - 高いモビリティ
  - 協調分散処理環境
- 曼陀羅システムの構成要素
  - 全学情報環境システム
    - システム全体を4分割し毎年更新
  - 電子図書館システム
    - システム全体を2分割し隔年更新
  - 曼陀羅ネットワーク
    - 概算要求により、8年を目途に更新
  - 各部局独自システム
    - 各部局で独自導入



# NAIST曼陀羅




<2014年5月>

# 全学情報環境システム

- 個人用常用ワークステーション
  - シンクライアント型
  - ネットブート型
- 共用サーバシステム
  - 大容量高速ファイルサーバ
    - 物理容量 約 6.3PB
  - 小規模計算サーバ
    - 大容量データ処理ノード
    - 広帯域分散ファイルサーバ
    - 大容量共有メモリノード
    - 超並列演算ノード
    - クラスタノード(Blade型)
  - 共通基盤サーバ
- 特定研究用サーバ

ファイルサーバ(一部)

# 計算サーバ

- 自由に使える計算サーバ群
- 用途に応じた複数タイプの計算サーバ群を提供
  - メモリ重視：2TB 大容量共有メモリノード
  - CPU重視：20core 3.0GHz Xeon クラスタノード
  - 並列処理重視：GPGPU装備の超並列演算ノード
- 用途に応じた複数タイプのストレージ
  - 汎用アクセスの ZFS Storage Appliance
  - 分散高速アクセスのGluster FS
  - Hadoop 実行環境のBig Data Appliance
- 40GのInfiniBand または10GbEで相互に接続

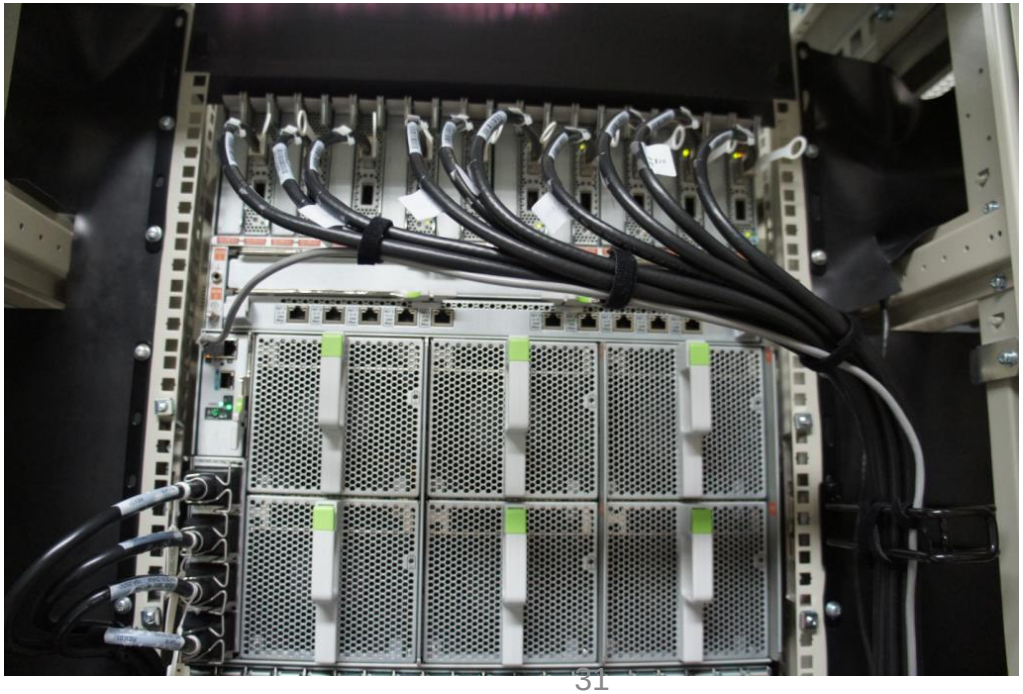
# 計算機リソース、ストレージ 4年間(H21からH25)の動き

| 項目 | H21導入システム | H25導入システム |
|---|---|---|
| 主ファイル サーバ | Sun Storage 7410 **276TB** | Sun ZFS Storage 7420 M2<br>Oracle ZFS Storage ZS3-2 **708TB** |
| クラスタファイル サーバ | Sun Fire X4540 **384TB** | Sun Server X4-2L **864TB** (Gluster FS) |
| | | Oracle Big Data Appliance **648TB** (hadoop HDFS) |
| 大容量共有 メモリノード | Sun Fire X4600 M2 x4台 **32core, 512GB**, NVIDIA Tesla | Sun Server X2-8 x2台 **80core, 2TB** |
| | | HP Proliant SL6500 x2台 NVIDIA Tesla |
| クラスタノード | Sun Blade X6270 x120台 **8core, 24GB** | Sun Blade X4-2B x120台 **20core, 64GB** |
| ジョブ管理 | Sun Grid Engine | Open Grid Scheduler |
| インターコネクト | 10Gb Ethernet | 40Gbps InfiniBand |

たかだか1500名規模の組織でも管理しなければいけない情報量は4年間で
ほぼ倍に増加。当然、それだけの情報保護、セキュリティ対策も必要に・・・

# 集中管理の効率化もセキュリティの一貫

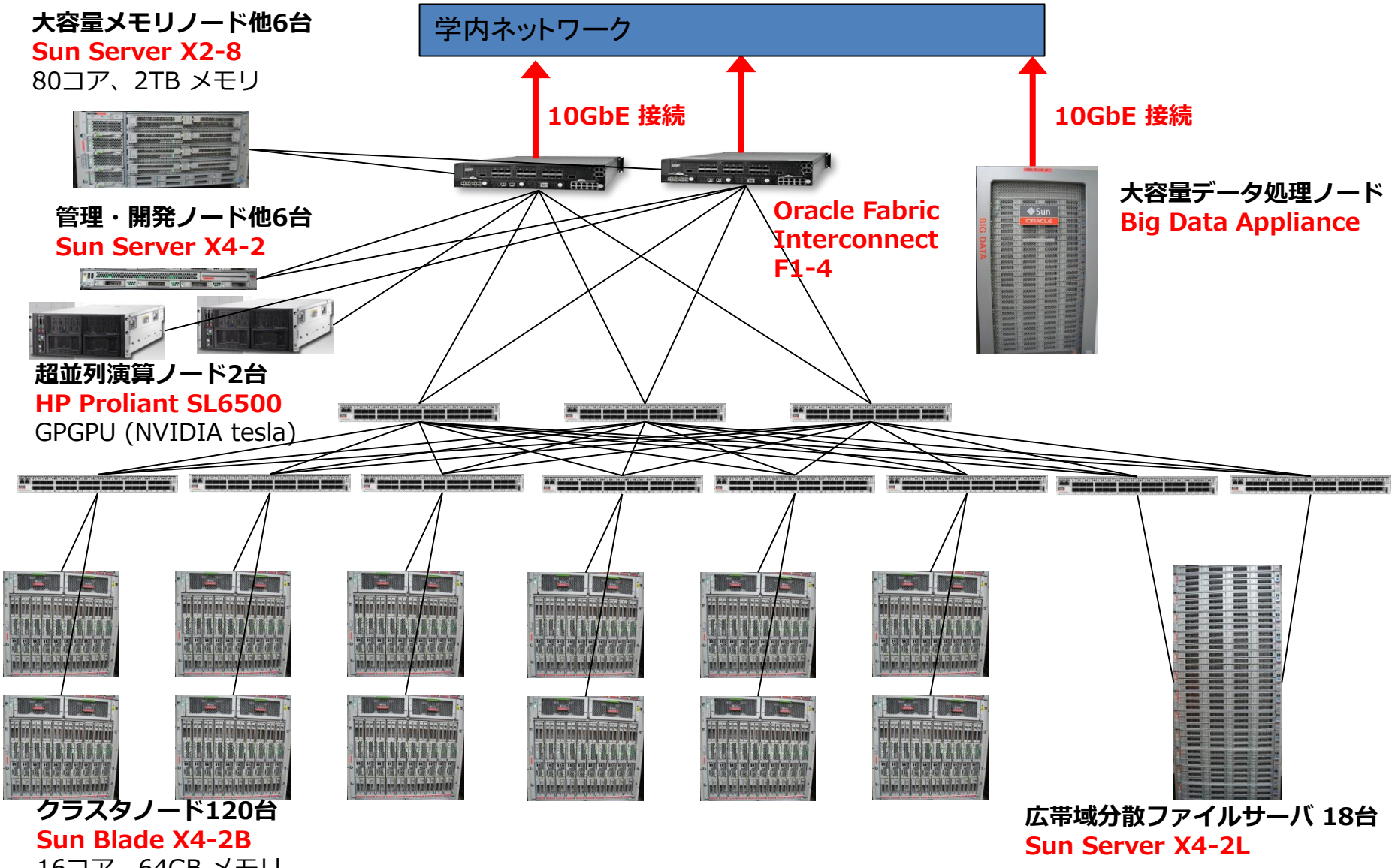
- 150台の計算サーバ群を管理するInfiniBandスイッチ
  - 40GbpsのInfiniBandケーブルに、仮想的にEthernetを作成し、計算サーバ群の内部やスイッチ外部とも通信
- 集中管理の効率化（セキュリティ対策の一例）
  - 仮想Ethernet 経由でのPXEブートで計算サーバ群のOSイメージを集中管理



すっきりとしたケーブリングで
サーバブレード毎にInfiniBand１本だけ(セキュリティ視点から重要)

InfiniBandを使用しながら、仮想Ethernetを同時に使用可能

# 計算サーバ相互接続ネットワーク



# 授業コンテンツの著作権

- 機能
  - メディアセンター
    - 雑誌・図書・動画などのコンテンツ配信機能
  - 高度な情報検索
    - 書誌・目次・抄録情報のみではなく本文情報を検索対象
  - 授業アーカイブ
    - 許諾を受けた授業（講師）のみコンテンツとして収録・配信
    - 遠隔配信講義は特に要注意
- 主要システム
  - 検索システム
  - デジタルビデオシステム
  - アカデミックチャンネル
- 地上波デジタル放送
  - チャンネル枝番の活用

| | | |
|---|---|---|
| 8 | 081 | 関西テレビ |
| 9 | 091 | 奈良テレビ |
| 10 | 101 | 読売テレビ |
| 11 | 111-1 | ミレニアムホール |
| | 111-2 | 図書館 マルチメディアホール |
| | 111-3 | 先端科学技術研究調査センター 研修ホール (*) |
| 12 | 121-1 | 情報科学研究科 L1 大講義室 |
| | 121-2 | 情報科学研究科 L2 講義室 |
| | 121-3 | 情報科学研究科 L3 講義室 |
| | 121-4 | バイオサイエンス研究科 大講義室 |
| | 121-5 | 物質創成科学研究科 大講義室 |

# 大学におけるBCP化

- NAISTクラウド
  - リソースは（学生・教員）が欲しいときに欲しいだけ
  - リソース(ハード・ソフト)の集約化（管理の一元化）

- 学内クラウドサービス
  - IaaS
    - ハードウェアの貸し出し
  - PaaS
    - 仮想計算機VMの貸し出し
  - SaaS
    - サーバソフトウェアの貸し出し

- 研究活動は24時間365日。優れた成果物を生み出すためには計算資源の常時稼働は不可欠

# 集約化とそのリスク

- ハードウェアの集約化
  - ファシリティ強化が急務（リース問題も考慮する必要あり）
    - 予算が必要
    - 意義の明確化

NAIST ITCのBCP策定

- NAIST BCP策定ポイント
  - 緊急時対応(大規模なインシデント発生を想定）
    - リソースの洗い出し・復旧優先順位の決定
    - 緊急連絡網（縦割りから横のつながりへ）
  - システム脆弱性の洗い出し
  - PDCAの徹底
- 仮想計算機管理の難しさ
  - 学生・教員は自由にサーバを立てたがる、そして放置…（汗

# コンテナ型サーバ収容設備

- ファシリティ強化の一環
  - 可用性の強化
    - 外部環境に応じた空調（冬は寒い）
    - 沖縄科学技術大学院大学 (OIST) とのDR連携
    - 非常時における衛星通信利用
  - 免震設備
  - セキュリティ対策
    - 監視カメラ(設備内外)
    - 入退室管理システム
  - グリーンIT
    - 電力・温度・湿度センサ
    - 太陽光パネル

建築物ではない
固定資産税、減価償却の軽減
耐用年数後に廃棄可

# コンテナサーバ収容設備内部

42Uラック

電源レールとブレーカー

ブレーカー

# 大学システムの「見える化」の実装例

【コンテナ側機器】
- 環境監視システム
- 負荷装置---サーバ監視／カメラ
- PoE機器

## 1）ソーラー発電システム

フィルム型（6枚）

パワコン

ソーラー構成

＊屋根に設置

AC

## 2）モニタリングシステム

センサー

見える化

日射計
気温系

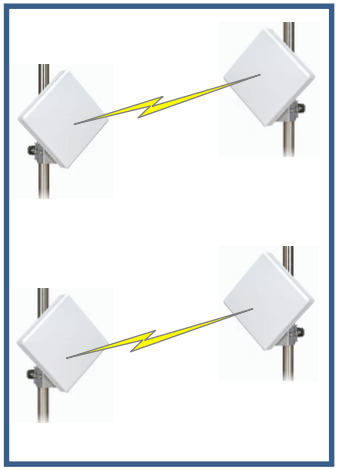
監視処理

充電器
(UPS)

AC100V

＊パワコン、監視処理：前室に設置
＊センサー：ポールに設置
＊充電器：ネットワークーラックに設置

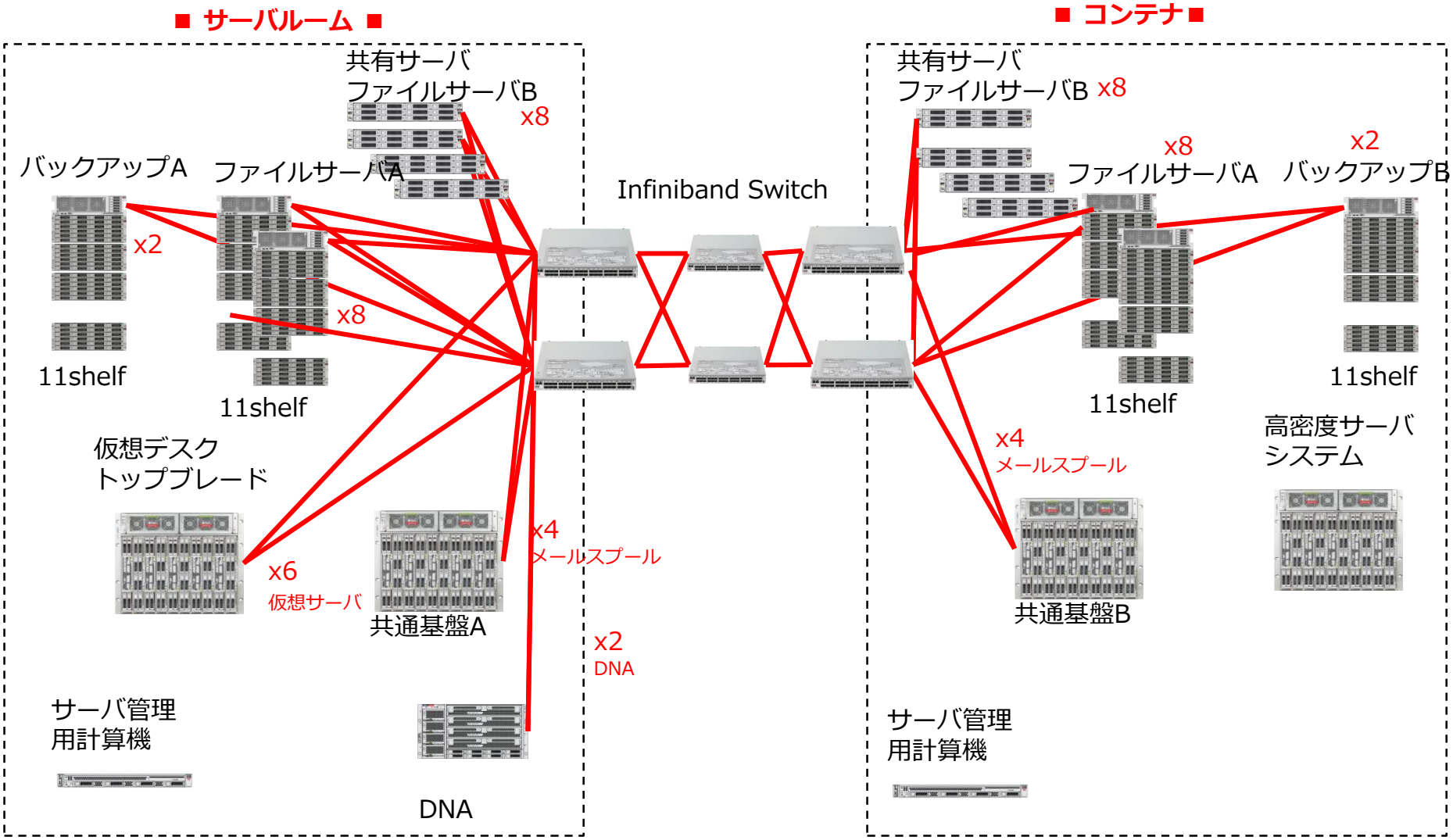
## 3）小電力無線データ通信システム



＊センサーと共にポールに設置
（2対向）

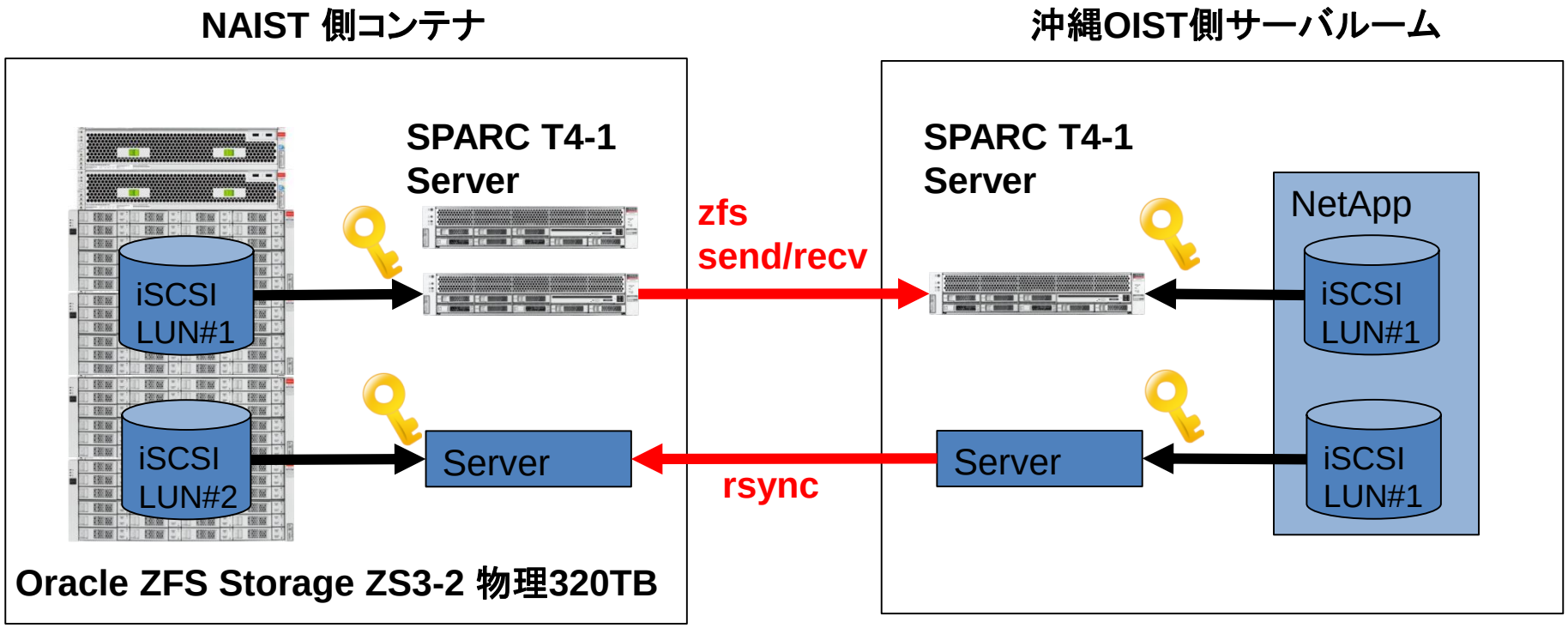
**ポール位置**
＊．ポールは基礎に固定せず自立設置

# コンテナサーバ収容設備による可用性強化




**Infiniband Switch 間は、200m の光ケーブルで接続**

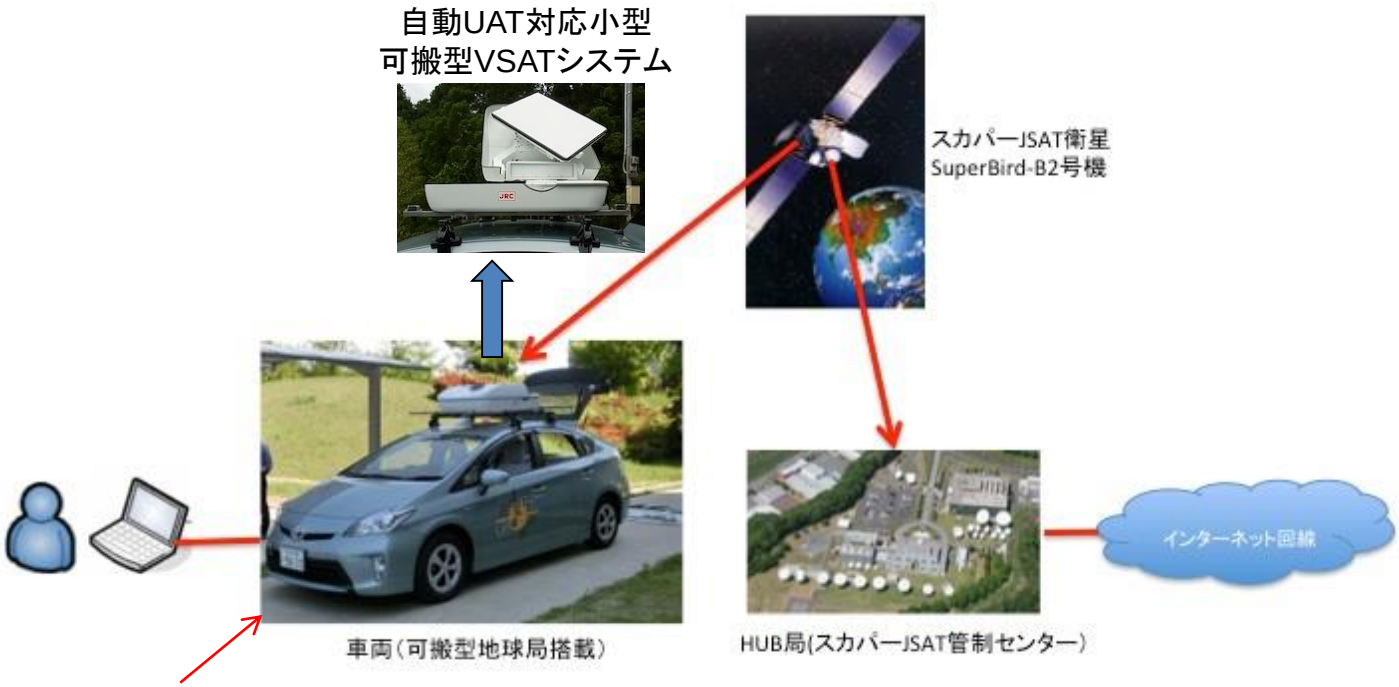
# 冗長性の良さとリスクは何だろうか
# 距離的にも離れた沖縄




- データは、SPARC/Solaris のzfs send/recv コマンドでスナップショット間の更新差分だけを効率的に送受信し、転送量を削減
- 丸ごとバックアップデータの冗長化の利点とリスク
- 管理者がデータを見れないようにするため、ストレージは iSCSI ブロックデバイスを提供しサーバ側でファイルシステム暗号化を実施
- SPARCサーバでは、SPARCプロセッサ内蔵暗号処理チップにオフロードし、性能向上およびCPU利用率削減

# アドホック型衛星インターネット通信システム

- 大規模な災害発生や非常時等
  - 地域への通信インフラ提供
  - 現状の問題は衛星回線のコスト

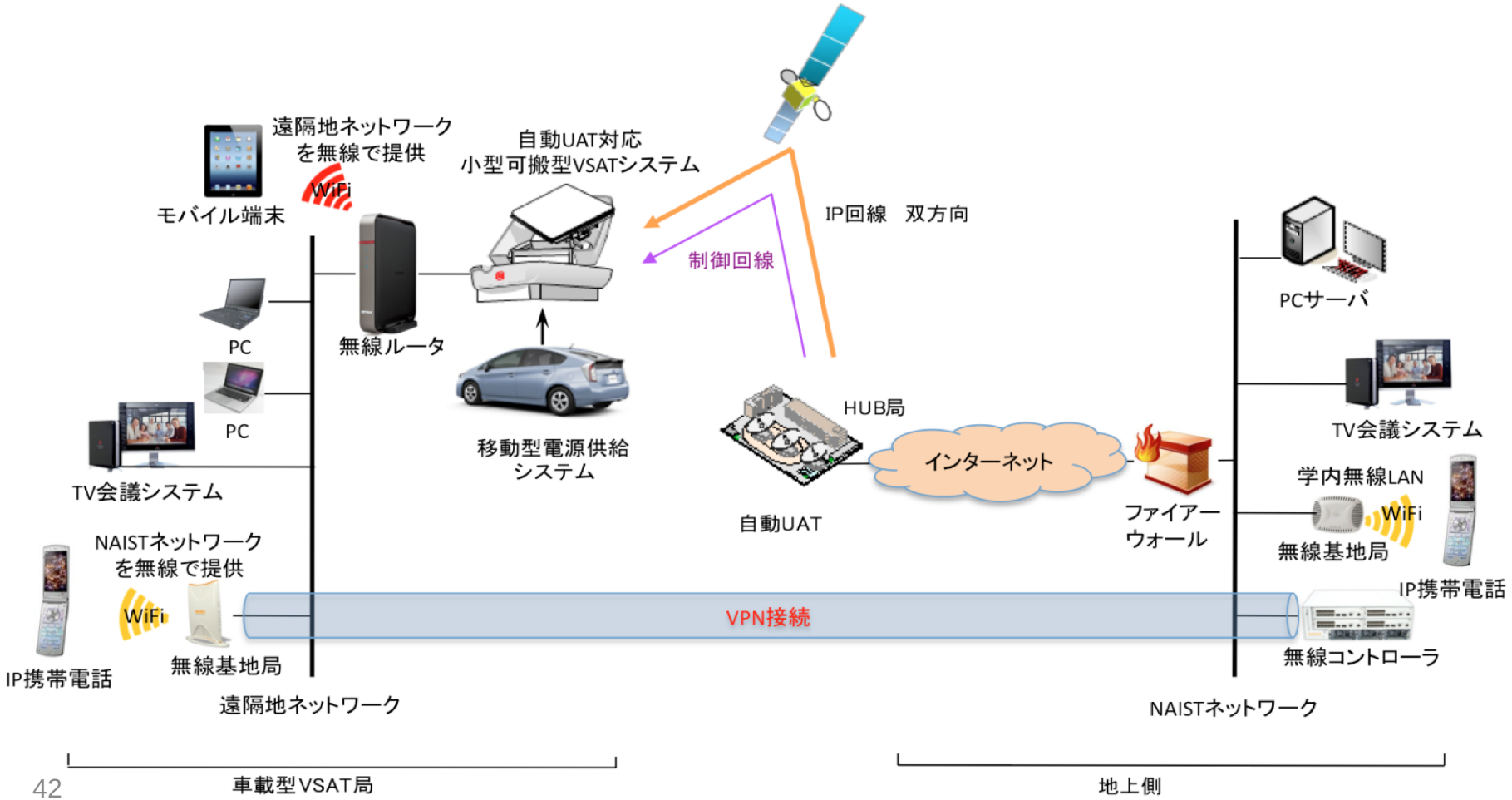





世界初の自律式車載型衛星通信システム

# アドホック型衛星インターネット通信システム

- 非常時における通信回線の冗長化
- データプレーンとコントロールプレーンの分離



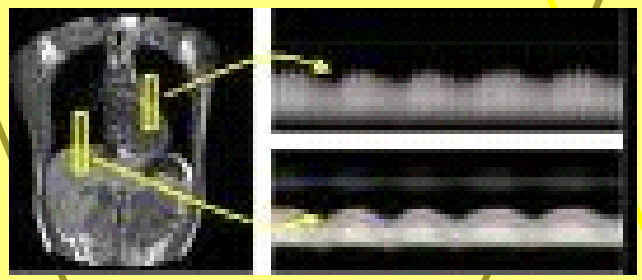
# 私たち大学が守るべき個人情報と研究データ（資産）

- 大学と企業の大きな情報管理の違い
  - 個人情報を扱うことはあまり無い←意識の薄れ、欠如
    - 答案用紙や学生名簿の気軽な持ち出し
      - USBデバイスの停止はありえない
      - Excelも（マクロも）やり取りは当たり前
  - 特許や未発表の研究成果、実験データ
    - 大型計算機で日々出力される膨大なデータ保管先
      - 最近は数TB管理が容易なテープドライブへ
  - ゲノム（遺伝子や染色体）情報や医用情報
    - 共同研究先や医療機関から届けられた機微情報（氏名が削除された加工データとはいえ、年齢・性別・身長・体重・血糖値、等の非常にセンシティブな情報）

# 機微情報の例（前臨床研究）

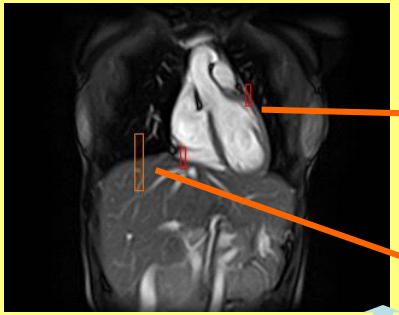
MR

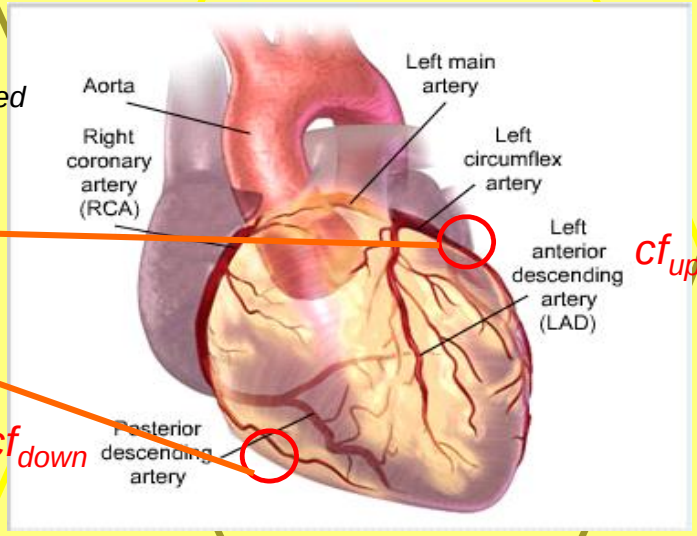
Motion correlation:
Right Diaphragm Upper
Right Diaphragm Lower



Navigator tracking of diaphragm in the SI direction

*For initial studies, SSFP scans are used*



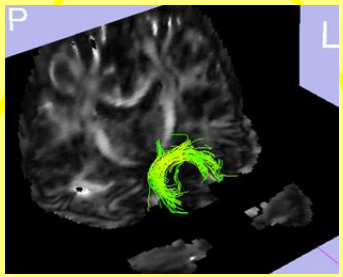




医用画像処理による冠動脈撮像時の動き補償
MRI を用いた冠動脈検査の支援

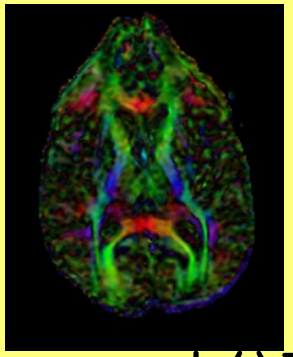
## 医用画像等における画像処理

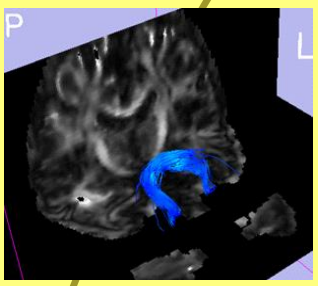
# 機微情報の例（前臨床研究）

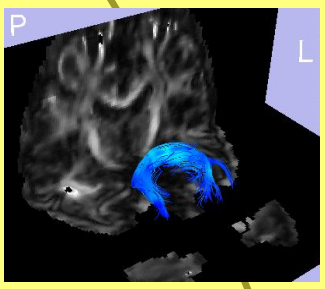
MR

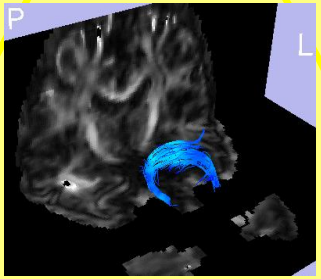


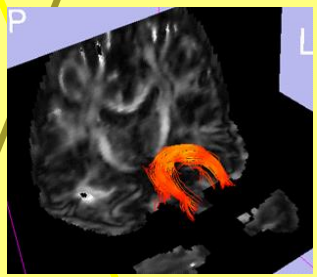

Template

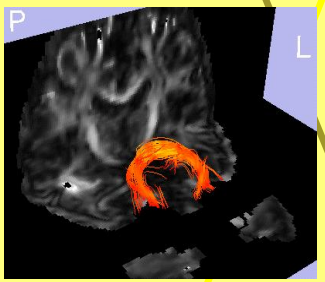


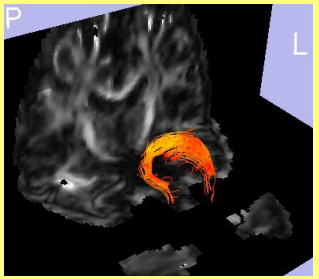


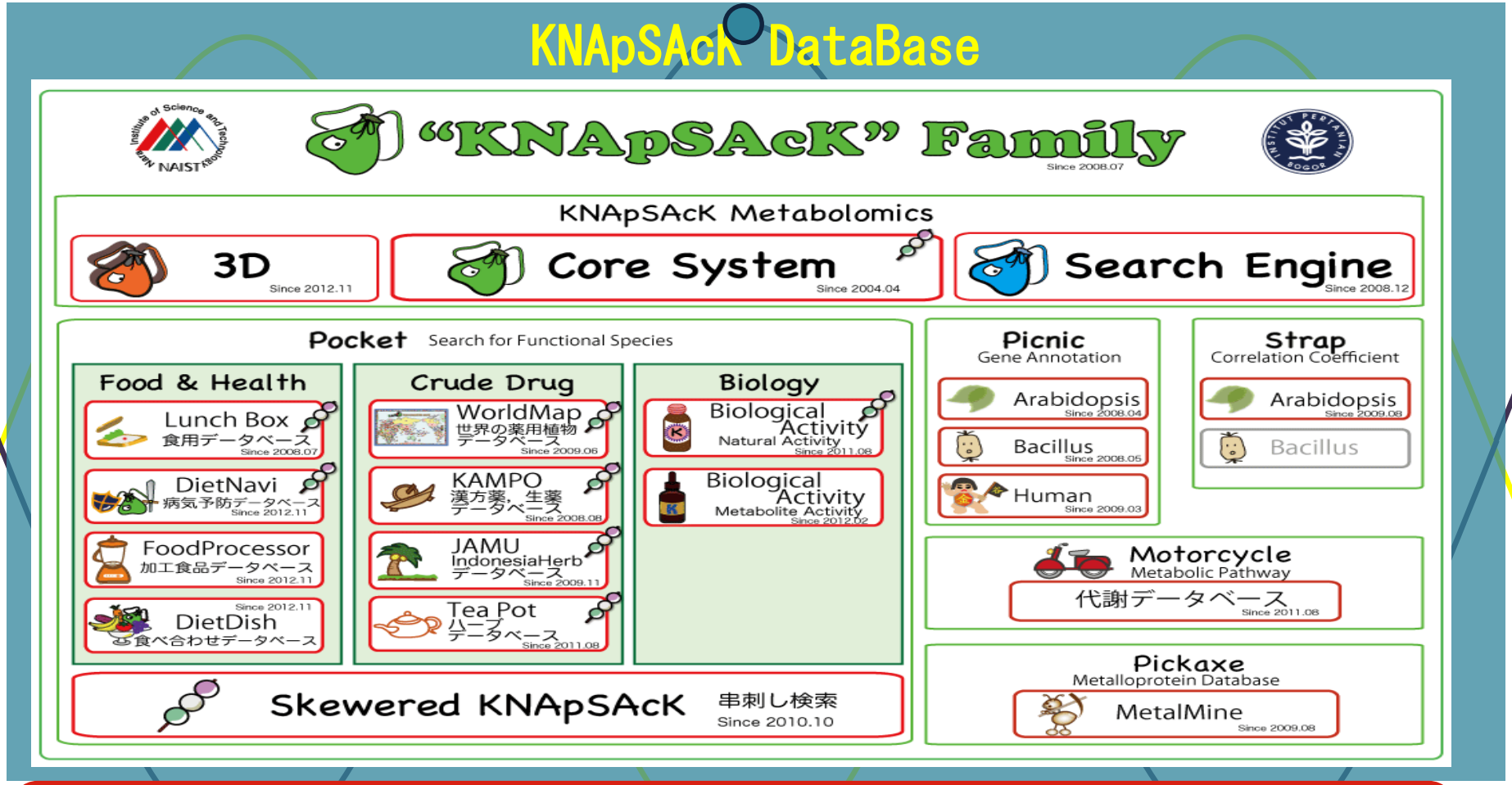




- 水分子の拡散による微小移動を計測（拡散テンソル）
- 神経・筋線維走行を追跡する新しい画像処理の研究

**画像処理**

# データベースの例（天然化合物）




メタボロミクスによる食物あるいは生薬としての、植物のヒトへの効果を分子レベルで解明するためにの「生物-代謝物データベース」

# データベースの例（天然化合物）

## KNApSAcK DataBase

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| マグロ | 1 | 黒糖 | 3 | コメ油 | 5 | 魚類 | 8 | ココナッツ | 38 |
| ワカメ | 1 | スパイス | 2 | アマランサス | 1 | シメジ | 7 | ヨーグルト | 27 |
| L-グルタミン酸Na | 1 | ウナギ | 2 | アワ | 1 | 魚醤 | 6 | 赤ワイン | 35 |
| 5'-リボヌクレオタイドNa | 1 | 日本茶 | 3 | インゲンマメ | 1 | コンブ | 6 | 加工澱粉 | 30 |
| | | 色素 | 2 | ヒエ | 1 | 発酵調味料 | 9 | ブイヨン | 26 |
| 雑肉 | 1 | ビタミンC | 4 | カボチャ | 3 | シナモン | 6 | セロリ | 23 |
| ピンダルーペースト | | ビタミンE | 3 | シジミ | 2 | クローブ | 3 | ハチミツ | 24 |
| | 1 | サクランボ | 1 | 油脂 | 3 | フェンネル | 2 | トウガラシ | 23 |
| トウモロコシ | 1 | ラック色素 | 1 | アオマメ | 2 | ナツメグ | 2 | ガラムマサラ | 11 |
| 果実ミックスジュース | | 牡蠣 | 5 | キビ | 1 | ホタテ | 9 | 米酢 | 15 |
| | 1 | ショ糖脂肪酸エステル | 5 | オクラ | 1 | シイタケ | 7 | カルダモン | 7 |
| 貝類 | 1 | ナス | 4 | オオムギ | 1 | ウコン | 5 | クミン | 14 |
| カルシウム | 1 | ごま油 | 2 | 香味野菜 | 3 | ピーマン | 2 | コリアンダー | 11 |
| アコヤガイ | 1 | タケノコ | 3 | サバ | 4 | キャベツ | 2 | フォン・ド・ボー | 16 |
| 鹿肉 | 1 | ローリエ | 2 | 煮干し | 3 | バジル | 1 | コショウ | 13 |
| 牛すね肉 | 1 | スイカ | 1 | クコの実 | 5 | エリンギ | 4 | 粉末ソース | 7 |
| ベシャメルソースベース | 1 | ヤマイモ | 1 | テンサイ | 2 | レモン | 3 | トウモロコシ油 | 10 |
| | | パセリ | 1 | ラ・フランス | 2 | ヒラタケ | 1 | コンソメ | 12 |
| アメリケーヌソース | 1 | スクラロース | 4 | ピーナッツ | 3 | ポピーシード | 1 | 酒 | 14 |
| アシタバ | 1 | リン酸塩Na | 3 | だし | 3 | 綿実油 | 9 | 乳糖 | 19 |
| 納豆 | 1 | ランチョンミート | 1 | トレハロース | 2 | 乳酸 | 5 | コーヒー | 10 |
| イチジク | 1 | 亜硝酸Na | 1 | フェヌグリーク | 1 | クエン酸 | 5 | 鰹節 | 11 |
| ローズマリー | 1 | ホウレンソウ | 2 | ステビア | 3 | ビタミンB2 | 3 | デキストリン | 12 |
| ヘッド | 1 | レタス | 1 | アジ | 1 | イカ | 7 | ダイズ | 11 |
| カレイ | 1 | ラッカセイ | 1 | タラ | 1 | エビ | 6 | カツオ | 12 |
| シシトウ | 1 | キウイ | 1 | コンニャク | 3 | アサリ | 2 | 水飴 | 7 |
| クロマメ | 1 | サザエ | 2 | サトイモ | 2 | 白ワイン | 3 | ソースパウダー | 6 |
| 液糖 | 1 | 牛ひき肉 | 3 | 水酸化カルシウム | 1 | 酢 | 7 | イワシ | 5 |
| アゴ | 1 | オレンジ | 3 | 焼肉ダレ | 2 | パイナップル | 5 | 中濃ソース | 17 |
| レンズマメ | 1 | 猪肉 | 3 | ソルビット | 1 | モモ | 4 | タマリンド | 11 |
| テンチャ | 1 | ブラウンルー | 2 | 動物油脂 | 6 | ミカン | 3 | 野菜 | 19 |
| アオジソ | 1 | セルロース | 2 | ゴマ | 4 | オリーブ油 | 4 | カンゾウ | 16 |
| メロン | 1 | トウガン | 2 | カカオ | 3 | シーズニング | 6 | フルーツチャツネ | 15 |
| ゴーヤ | 1 | アーモンド | 2 | メタリン酸Na | 1 | オリーブ葉茶 | 3 | マーガリン | 10 |
| ノリ | 1 | ゼラチン | 2 | レシチン | 2 | ホワイトルー | 8 | 味噌 | 9 |
| コラーゲン | 1 | クジラ | 2 | カシューナッツ | 5 | みりん | 7 | カロチノイド | 8 |
| マイタケ | 1 | ユズ | 2 | タコ | 3 | ダイコン | 6 | パプリカ | 14 |
| 合鴨肉 | 1 | 牛たん | 2 | ウニ | 1 | 牛すじ肉 | 5 | クチナシ | 5 |
| ゴボウ | 1 | イチゴ | 2 | pH調整剤 | 1 | ネギ | 4 | ベニバナ | 4 |
| ヤーコン | 1 | ナシ | 2 | 柿 | 4 | 麹 | 1 | 増粘剤 | 7 |
| パルプ | 1 | 馬肉 | 2 | サツマイモ | 3 | ハクサイ | 1 | クラスタマメ | 8 |
| | | 米味噌 | 2 | レンコン | 3 | ニラ | 1 | キサンタン | 6 |
| | | アンズ | 1 | エノキ | 3 | ブドウ | 4 | ココア | 5 |
| | | アンニン | 1 | 豆腐 | 2 | ビール | 7 | サトウキビ | 4 |
| | | ポタージュ | 1 | 豆乳 | 2 | サラダ油 | 7 | キトサン | 5 |
| | | ベータカロテン | 1 | デミグラスソース | 4 | カニ | 5 | 3Aカルシウム | 3 |



Foods & Food Ingredients J. Jpn., Vol. 218, No.1, 2013

Cuisine Omics: Fundamental Structures of Zouni and Retortable Pouched Pack of Curry Unveiled by Multivariate Analysis Based on Food Ingredients

**料理のオミックス－食材からみえてくる雑煮とレトルト・カレーの構築原理**

桂樹 哲雄 (Tetsuo Katsuragi)　小野 直亮 (Naoaki Ono)　森田(平井) 晶 (Aki Hirai-Morita)
中村 由紀子 (Yukiko Nakamura)　Md. Altaf-Ul-Amin　金谷 重彦 (Shigehiko Kanaya)
奈良先端科学技術大学院大学情報科学研究科計算システムズ生物学研究室
奈良県生駒市高山町8916-5
Nara Institute of Science and Technology, Graduate School of Information Science, Computational Systems Biology Lab.
8916-5 Takayama, Ikoma-shi, Nara 630-0192, Japan

## クラスタリング

# 起こるべくして起きた事案

- 大学ならではの自由でオープンなネットワーク環境
  - 何も通過させないFWで全てを囲むことは時には研究活動の大きな障壁
    - 研究に必要となれば(断れない)グローバルIPアドレスの提供、DMZ設置等
  - 設定した人以外分からない多くの謎システム（kernel改変、FWルール等）
- セキュリティリテラシを学んでいない教員が多いことはもはや当たり前（上原先生の叫びも聞こえてきそう・・・
  - インシデント発生の対応の遅さ
  - 状況の深刻さの認識不足
  - 他人任せ、学生任せのWebサーバ、脆弱性のあるCMS
  - 忘れ去られ放置されたサーバ、PCの存在
- まずはFWのログを見てみましょうか（本邦初公開の非公開データです・・・）

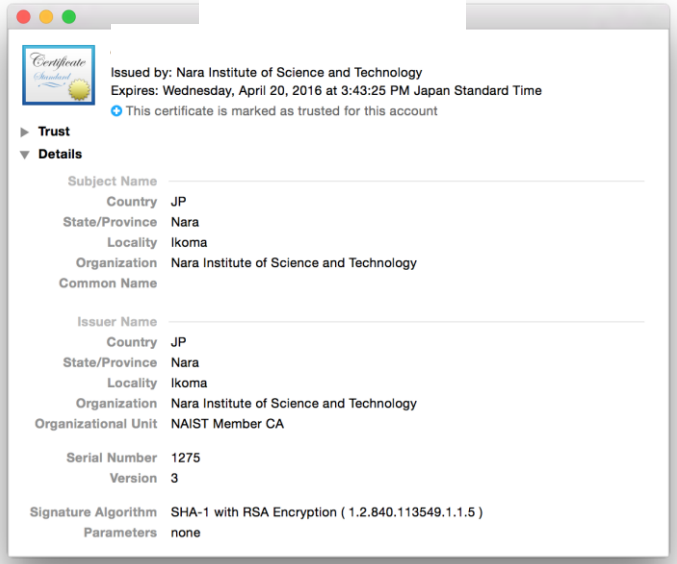
# NAISTにおける
# セキュリティインシデント対応フロー

- 緊急対応チームで状況把握
  - IDSシステムのアラート情報確認
  - ネットワーク切断、物理隔離、ログ保管等の処理
  - 関係教員への調査
  - 被害状況の整理、報告書作成、等
- 文部科学省様への届け出
- 県警様への届け出（被害状況による）

- 情報セキュリティに関わる教育の徹底化
  - 講習会を受講しなければ学内アカウントが有効化されない→（ある意味免許制？）効果あり

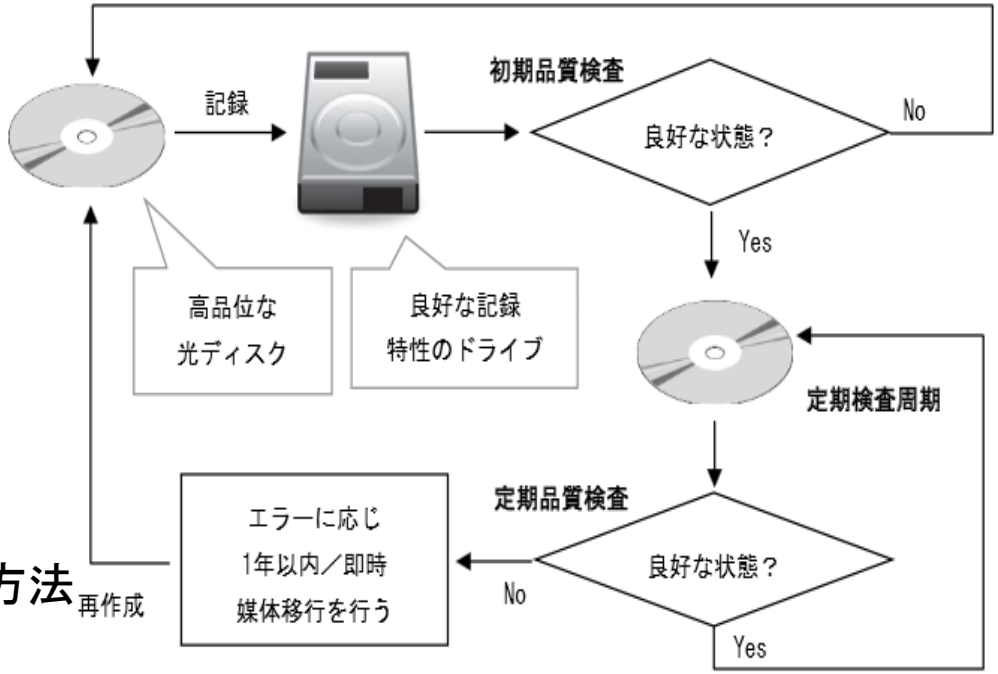
# 大学だからこそ考えるべき情報管理

- 長期に管理すべき膨大な電子化されたデータ群
  - 少なくとも30年は（研究によって得られた）中間成果物や実験データを適切に管理したい
    - データ以外に、学生さんの修了証明書や成績証明書は依頼がある限り発行する義務もある
  - センシティブな情報に対しては、本学クライアント証明書による署名付き暗号化
    - 電子データの長期保存?
    - まさに冷蔵庫の奥底



# 電子化文書の長期保存方法JIS Z 6017

- 2000年頃より情報の電子化により光ディスク等による電子化が進む
  - 2006年 JIS Z6017制定、2013年改定
  - BDへの対応
    - 基準ドライブと相関を確認したドライブの使用を推奨
  - 定期検査周期の見直し
    - 周期3年から5年へ（寿命推定30年）
  - 運用方法の簡素化
    - 3つの管理台帳から1本化へ




経済産業省「電子化文書の長期保存方法（品質検査フローチャート）より

# e-文書法

- 2005年4月の施行
  - 法的保存義務の文書の電子化データ保存への規制緩和
- 紙文書の電子化保存への要件
  - 見読性
  - 機密性(C)
  - 完全性(I)
  - 検索性
- 文書の原本性
  - 複製の容易さ
  - 内容の改ざん検知の困難さ
  - 作成日時の修正の容易さ
  - 長期保存でのリスク

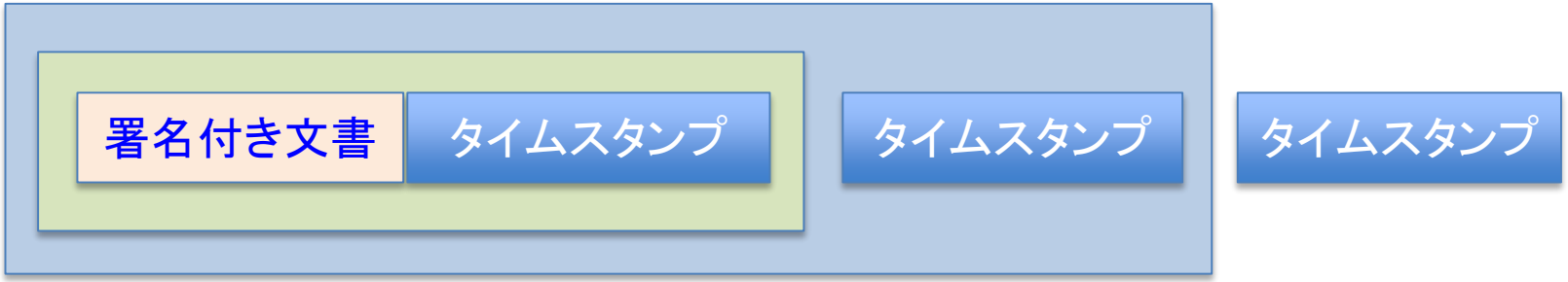
- 昨今の論文コピペ問題をきっかけに研究者モラルの低下

# 完全性要件

- 電子文書の原本性確認
  - 電子署名（だれが？）
    - 電子文書データの改ざん検知
  - タイムスタンプ（いつ？）
    - 信頼できる第3者による時刻認証
- 長期保管の問題
  - 有効期間後の真正性確認のための長期署名フォーマット
    - 欧州電気通信標準化協会(ETSI)により標準化、RFC3126
    - 次世代電子商取引推進協議会（ECOM）がJIS化
- 電子署名及び認証業務に関する法律（電子署名法）
  - 2001年4月施行
  - 電子署名がなされた電子文書は真正に成立したものと推定

# 長期署名フォーマットの必要性

- 「有効期間は有限」というどうしても避けられない問題
  1. 電子証明書（通常は1年ないし～3年ぐらい）
     - 有効期間が終了すれば保証も終了
  2. 署名タイムスタンプ（一般的に10年程度）
     - いつ署名が行われたかを示すタイムスタンプ
     - 証明書と比較して長く、長期保存に向いているが…。
  - 保管タイムスタンプ（有効期間の延長）
     - 10年越えはどうすべきだろうか
       - タイムスタンプが検証できれば良い
     - 暗号危殆化には耐えられるのか?
       - その時代で主流の強い暗号アルゴリズムを使えば良し



# 暗号危殆化はきっとくる～必ずくる～

- 大学ではできれば30年程度は電子データの保存をしていきたい。RSA-2048bitは(おそらく)30年は耐えるのではないか（猪俣の予測･･･汗
  - しかし、画期的な解読アルゴリズムが出たら、量子計算機がさくっと世の中に出てきたら･･･m(_ _)m
  - ケーススタディ
    - 時刻認証者(TSA)の秘密鍵が危殆化
      - TSAは速やかに対応する鍵の失効処理と新たな鍵への更新処理を実行
      - 対応する鍵を失効させたことをサービス利用者に通知、もしくは迅速な情報公開
    - タイムスタンプ署名時の秘密鍵が危殆化
      - TSAは当該秘密鍵で生成した全タイムスタンプトークンが無効になる→更新した別の秘密鍵によるタイムスタンプトークンを再取得する必要があることを迅速に利用者へ通知

# 大学における情報管理の悩み（オフレコでm(_ _)m）

- （割と）我がままな教員にセキュリティ意識を押しつけることはかなり困難、というか無理…。
  - まずは、小さなグループ（研究室）から学部学科、そして大きな組織（学校）の中でお互い同士を見えるようにすること
- セキュリティインシデントによる本当の脅威に対する希薄さ
  - 昨今の漏えい事件が引き起こした事の深刻さをしっかり認識することも大切
- 機密よりも機微なデータの取り扱い
  - 下手をすると組織が飛びかねない、常に高い意識をもつこと
  - もはや学長が頭を下げればいい話では無い
- 後身のため情報は少なくとも30年程は安全に管理したい
  - 暗号化したとしても、鍵管理を30年続けられる自信はあるのか

# enPiTセキュリティ分野(SecCap)も どうぞよろしくお願いいたします

- お気軽にご質問、ご意見くださいm(_ _)m
  - E-Mail： atsuo@itc.naist.jp　https://www.seccap.jp/
  - Facebook Atsuo INOMATA , SECCAPで検索


# 謝辞


- 奈良先端科学技術大学院大学
  - 総合情報基盤センター　辻井高浩助手
  - 総合情報基盤センター　情報基盤技術サービスグループ
  - 情報科学研究科　計算システムズ生物学　金谷研究室