

# サービスの継続性を担保する 電子カルテ秘密分散バックアップ技術の 研究開発

研究代表者: 木村映善 (愛媛大学)

愛媛大学・大阪大学・京都大学・福井大学・兵庫医科大学・NRIセキュアテクノロジーズ

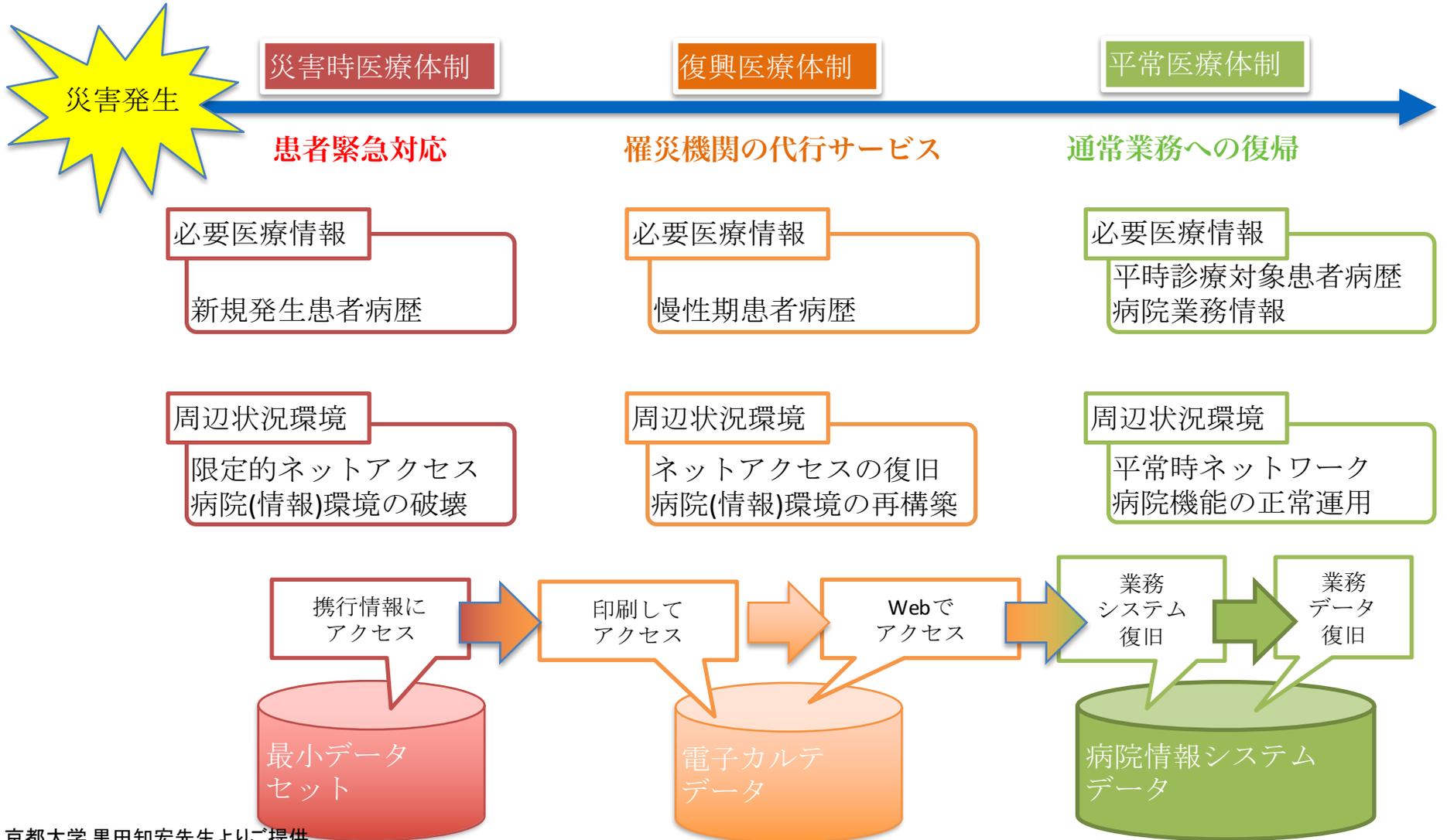


研究協力: アライドテレシス・NEC・日本IBM・日本電信電話・富士通・富士ゼロックス



# 本研究のターゲット

## —復旧ステージと必要となる医療情報—

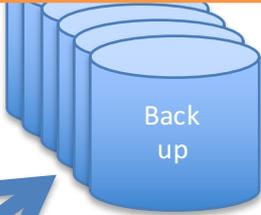


# 課題 電子カルテのバックアップ



安全のためには

多重リモート  
バックアップ



コスト  
がなあ

安くするには

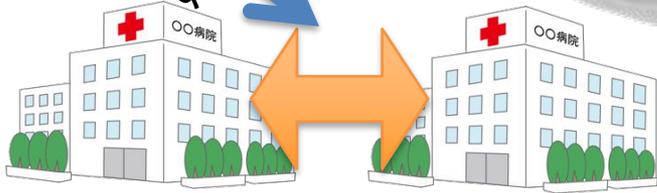


クラウドストレージ



安全性  
がなあ

安くするには

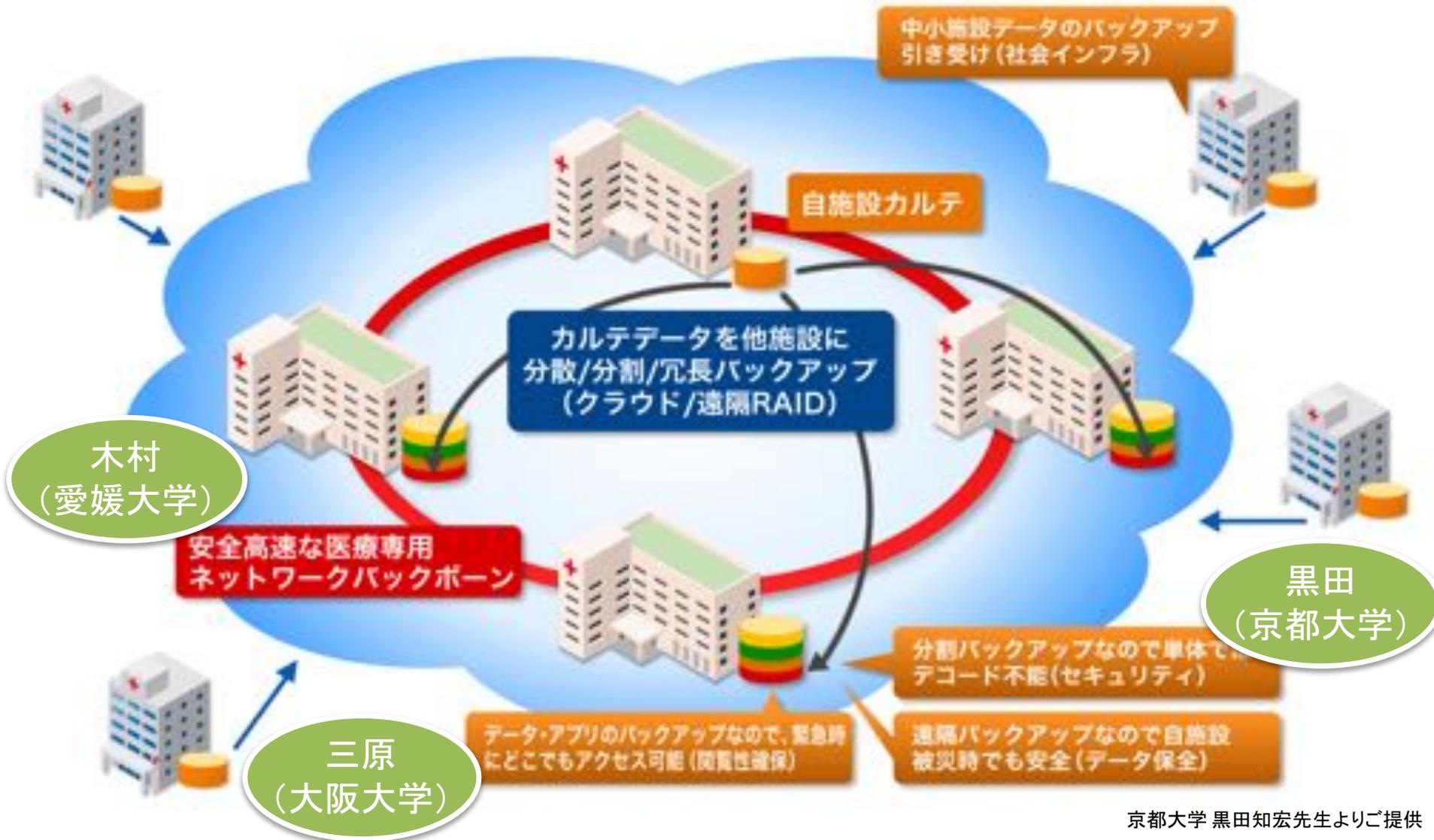


相互持合バックアップ



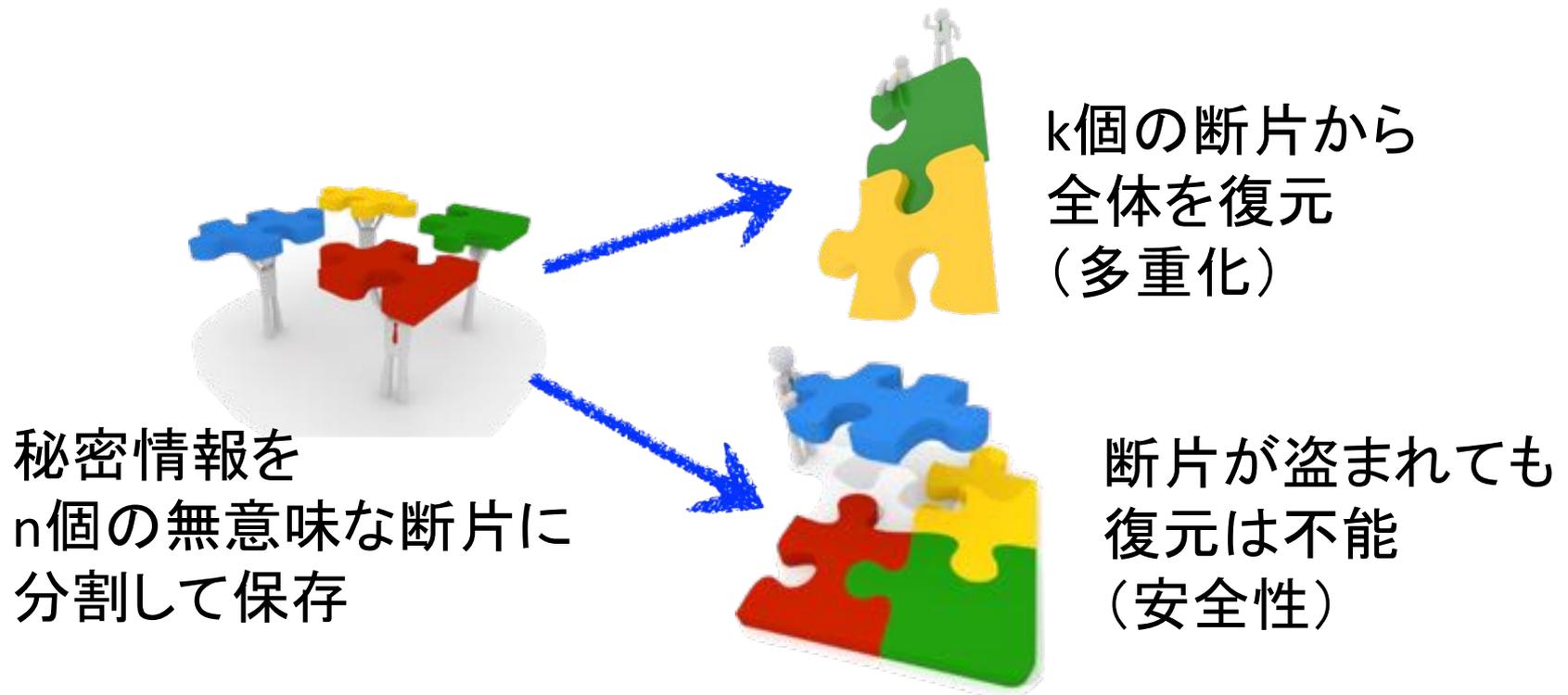
預かる  
責任が  
なあ

# 目指す未来：秘密分散バックアップ社会基盤



# 解決策

## (k, n) しきい値 秘密分散法



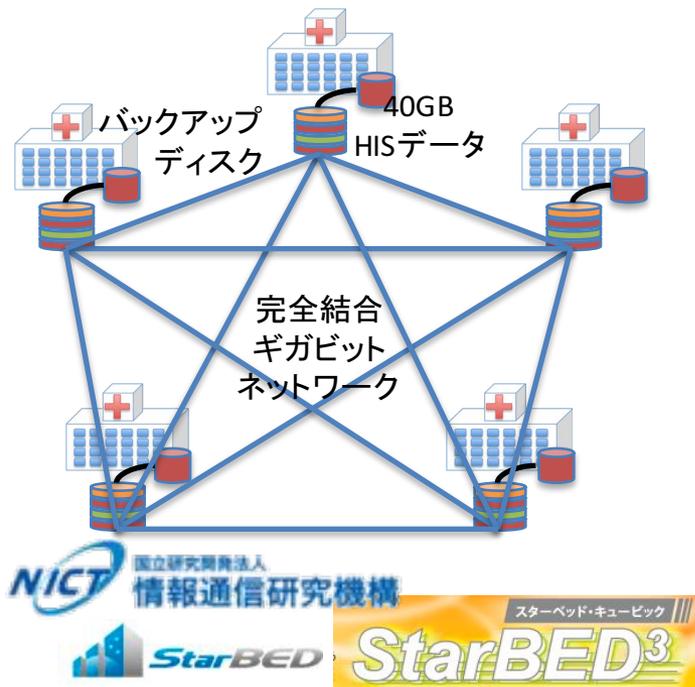
情報理論的暗号化してから送るので...

- 途中でデータをとられても安心
- 預かる側の責任も軽い

# 実験環境

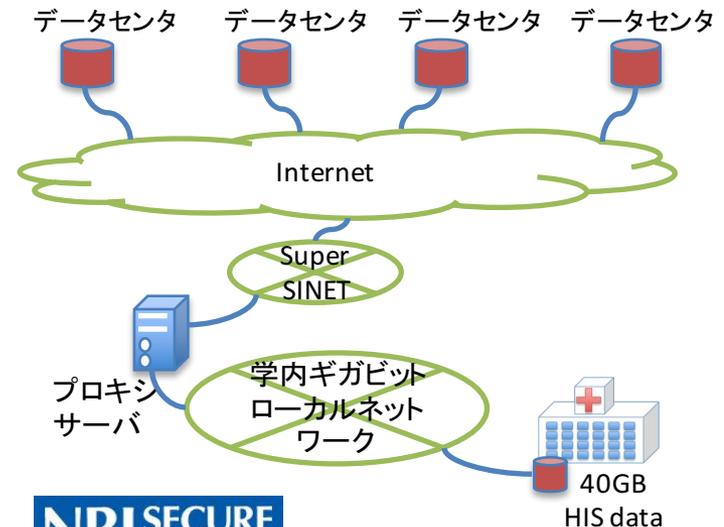
## シミュレーション

- 情報通信研究機構(NICT) StarBed3環境を利用
- 理想的環境を想定



## 商用サービス

- NRIセキュアテクノロジーズ SecretCube / SecretShareを利用
- インターネット環境を利用



NRI SECURE TECHNOLOGIES

SecureCube Secret Share

※40GBの電子カルテシミュレーションデータを利用

# 実験結果

- ネットワークの種類によらず実現可能
- 律速段階はOSのディスクI/O性能
  - ハードウェア的には8倍程度までは高速化可能

	通常時	被災時		復帰時
	分散保管	取り出し	再編成	再編成
シミュレーション	3:05:35	2:20:03	1:29:47	3:07:43
商用サービス	4:10:47	6:24:00		

# 紙カルテから電子カルテへ

紙カルテ



- 記録はシステムごとに分散保存される。
- 記録閲覧はサブシステムごとにViewerを起動する必要がある。

電子カルテ



基幹システム

経過記録・熱型表・院内紹介など



文書システム



スキャンシステム



放射線システム



生理検査システム

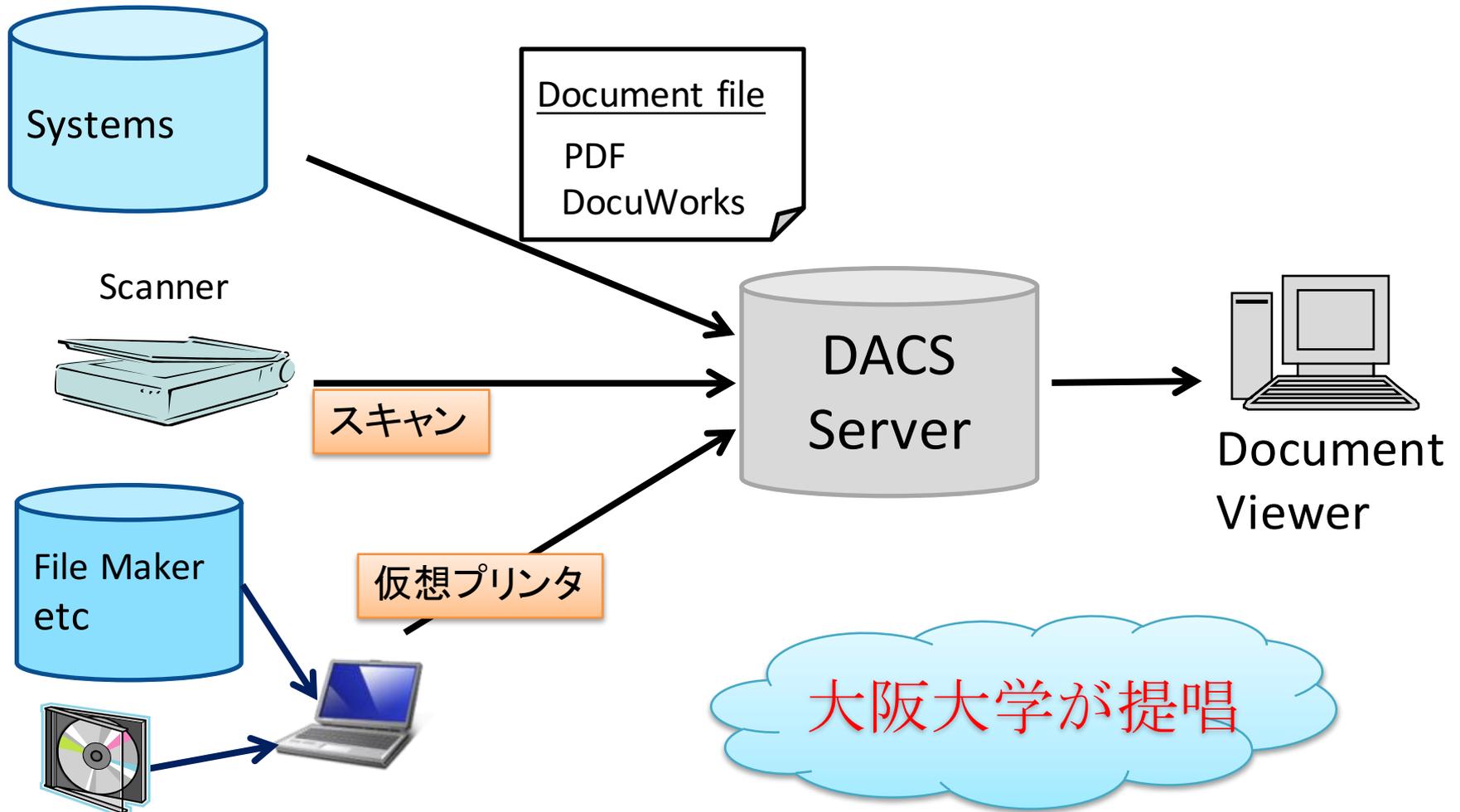


病理システム



# 診療記録文書統合管理システム

DACS (Document Archiving and Communication System)



# DACSによる診療記録の統合

## 電子カルテ



### 基幹システム

経過記録・熱型表・院内紹介など



文書システム



スキャンシステム



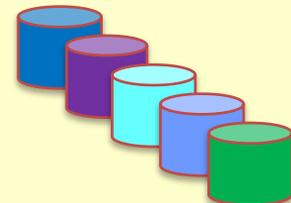
放射線システム



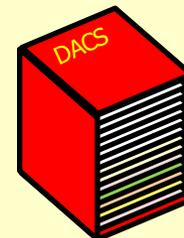
生理検査システム



病理システム



DACS



- 電子化により分散した診療記録を統合。
- 単一のViewerで、診療記録の閲覧が可能となる。

# DACS: Matrix Viewer

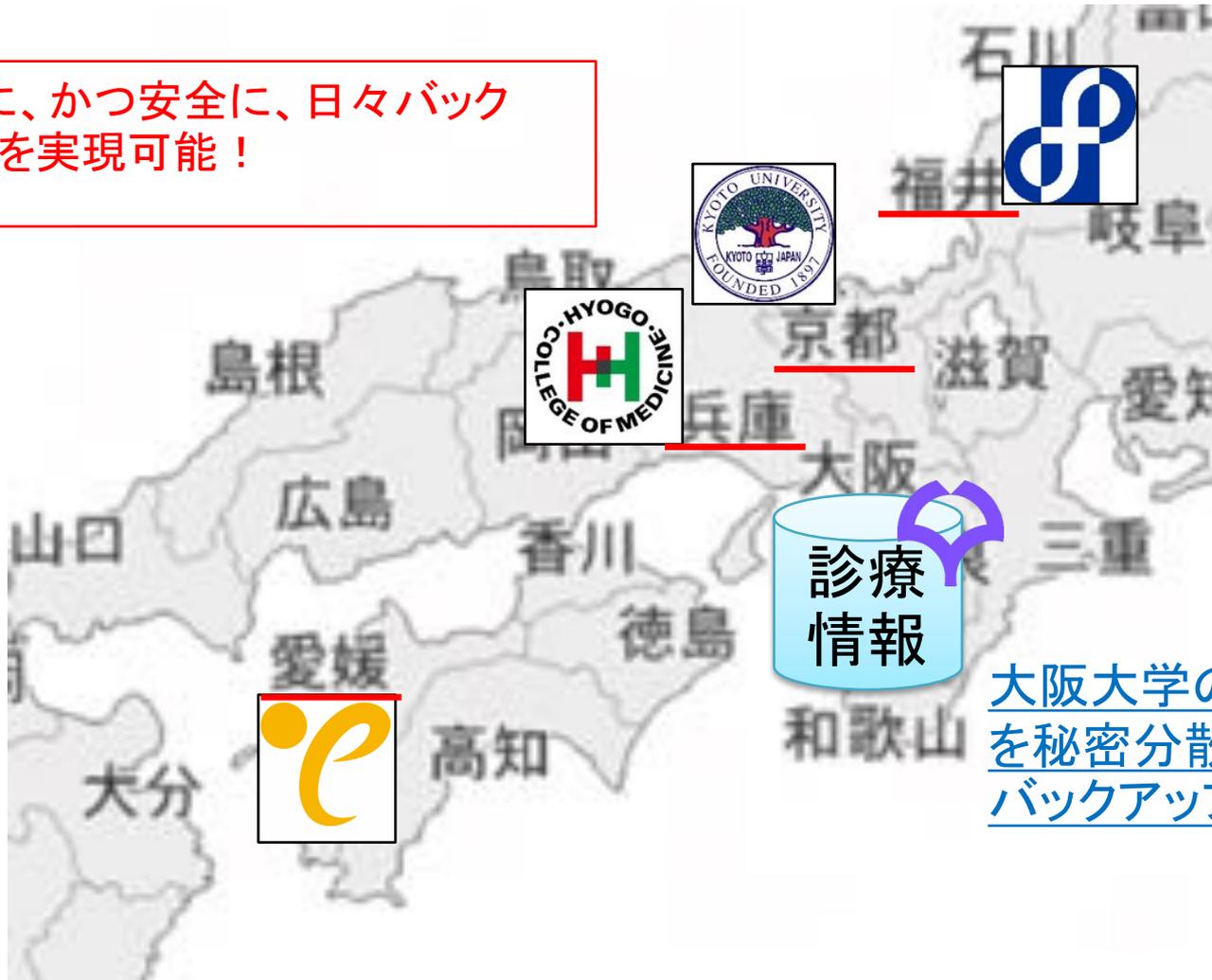


The screenshot displays the DACS Matrix Viewer interface. At the top, there's a header with 'MRV-MTX-1(1.1.4)' and 'システム情報'. Below this is a calendar view for the year 2011, with a red box highlighting a date in the 6th month. The main area shows a detailed view of a patient's schedule, with a red box highlighting a specific entry. A red arrow points from this box to a separate window showing a document viewer displaying a medical report titled '画像診断報告書 (第1版)'. The report contains various fields and text, including patient information and medical notes.

阪大病院では1つのViewerで全文書が  
閲覧可能

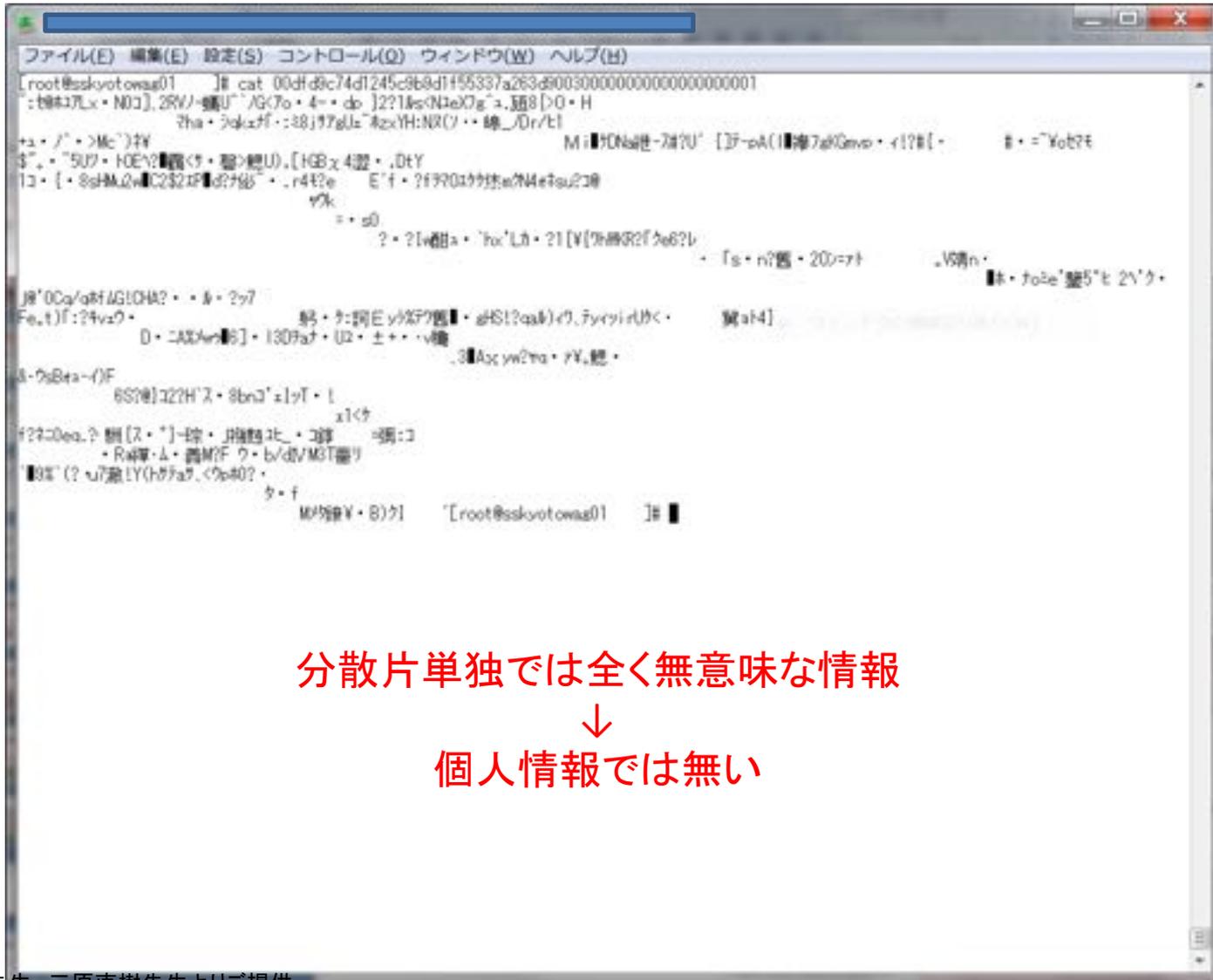
# 秘密分散バックアップ

安価に、かつ安全に、日々バックアップを実現可能！



大阪大学の診療情報を秘密分散技術でバックアップ

# 分散片ファイルの実際の中

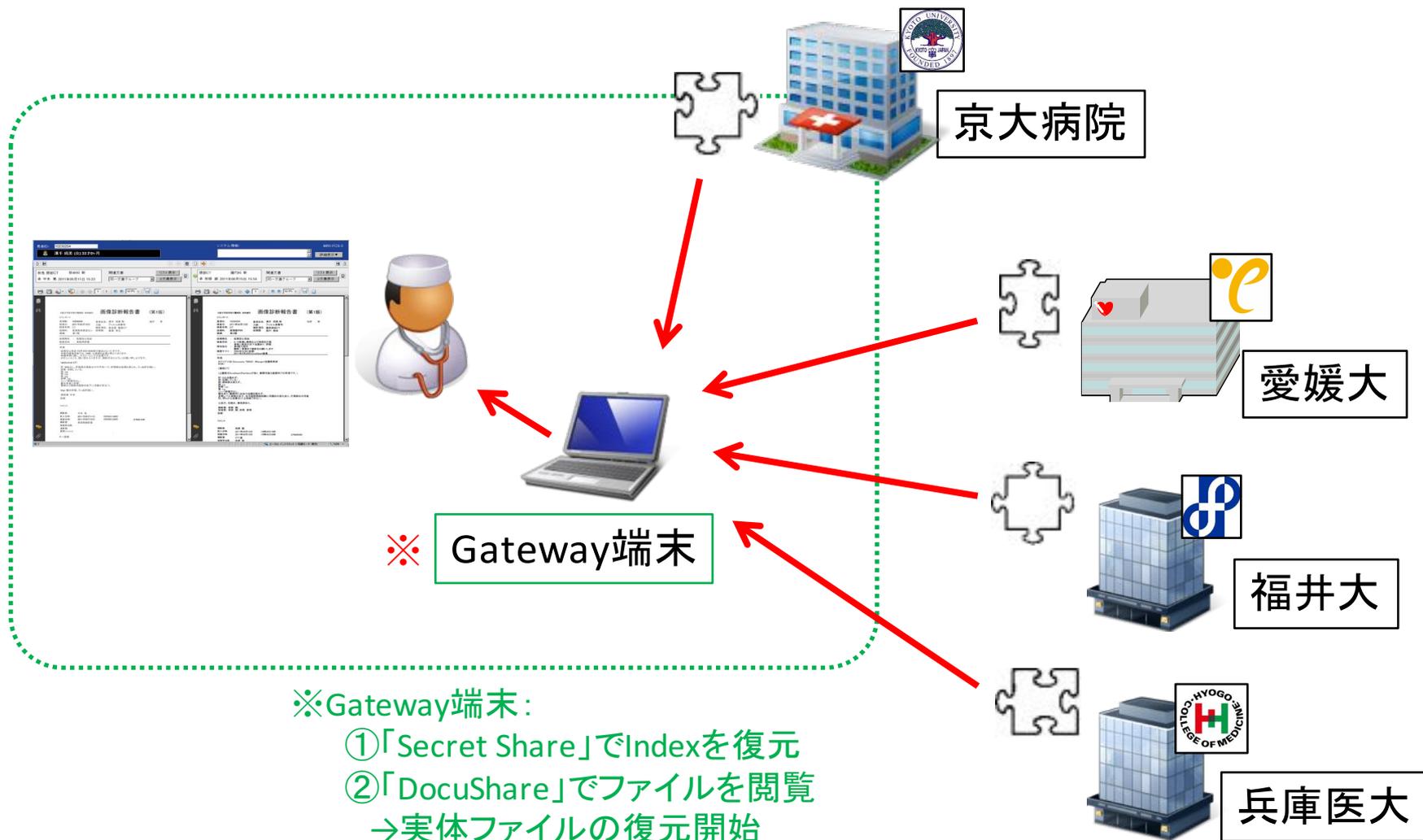


分散片単独では全く無意味な情報



個人情報では無い

# 京大病院での診療情報の復元

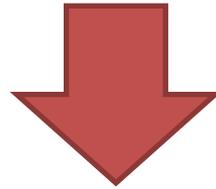


# まとめ

- DACSの技術を活用し診療情報を文書として保管することで、診療情報の統合管理が可能となる
- 秘密分散技術を活用することで、安全に低コストで診療情報を保管することができる
- 大災害時における診療情報の復元が可能

# これまでの災害に対する ネットワークの対策

- 冗長度を上げる
  - 様々なメディア・経路を活用する
- 復旧プロセスの迅速化



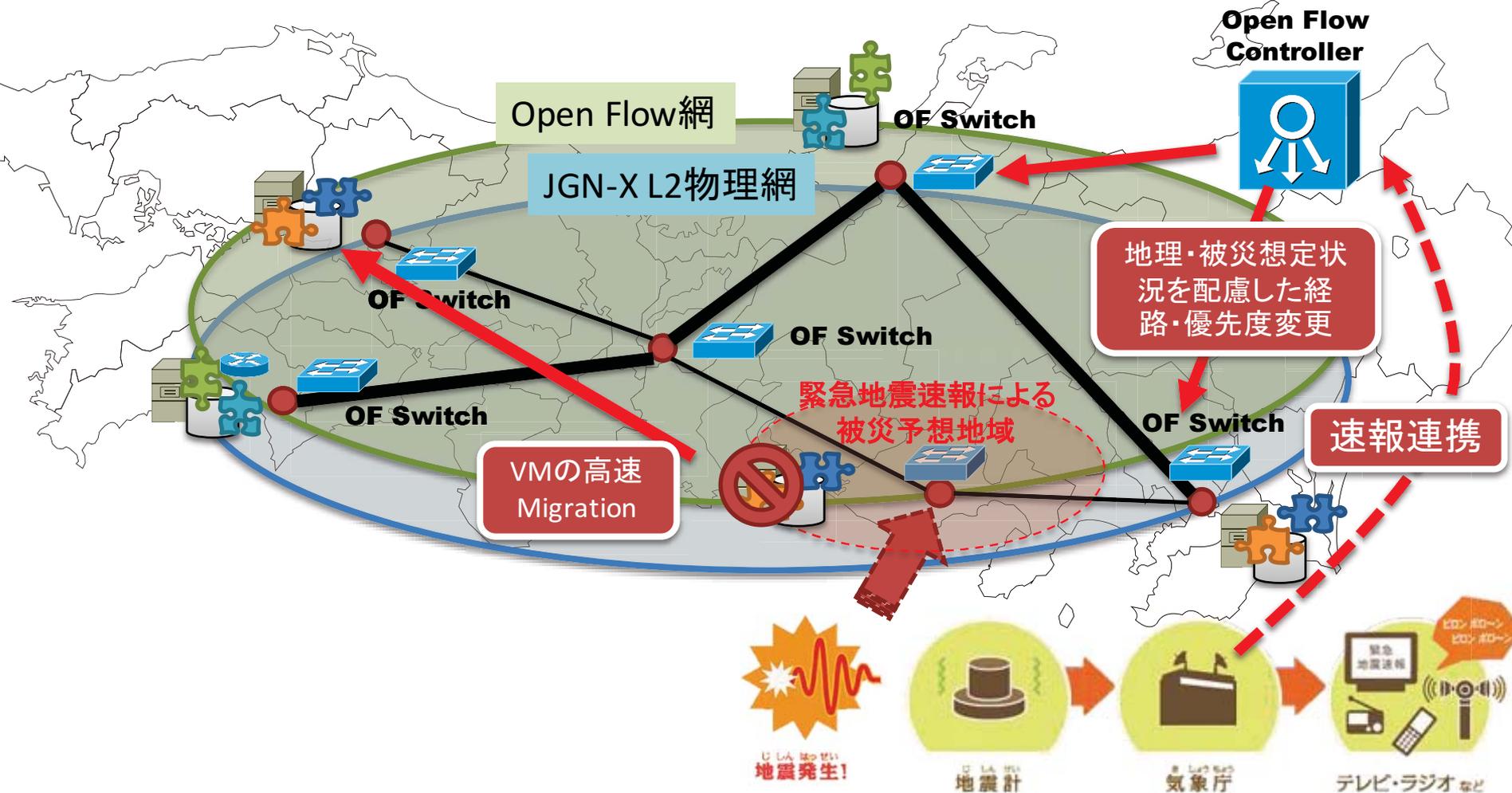
- いずれも、“事後対策”に特化
- 想定していない被害には対応できない
- ネットワーク事業者側に限られていた対策  
複雑な実装  
ユーザー側は何も手を打てない

# 発想の転換

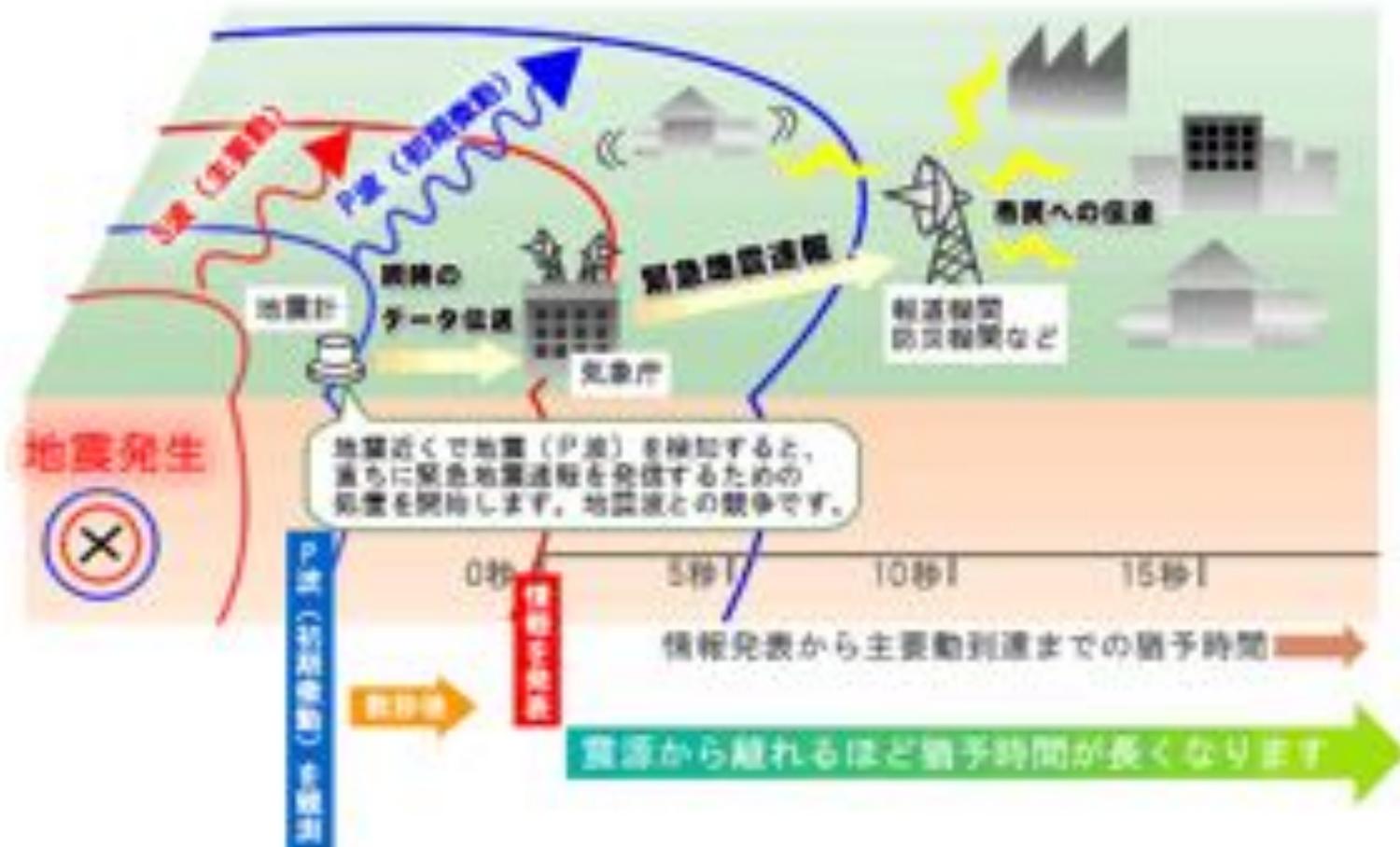
- ”事前に対策”できたなら？
    - Reactiveからproactiveへの変換
  - ユーザのリスク判断に応じて、  
ユーザーの意思で選択できたなら？
- ↓
- ユーザが容易にネットワーク制御できる  
環境を提供



# Open Flowと地震緊急速報連携による “Proactive Disaster Response”の実現

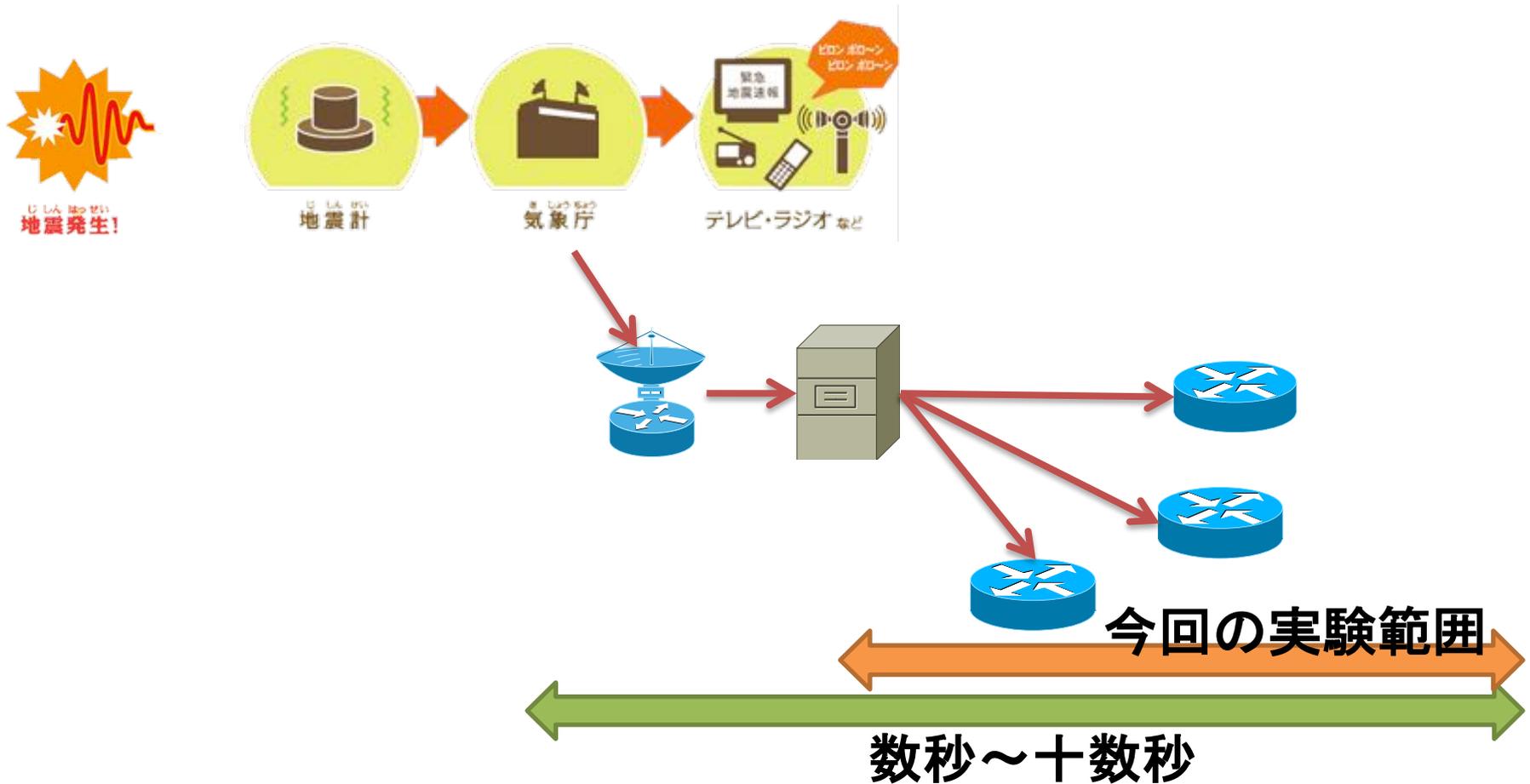


# 猶予時間は数秒～十数秒



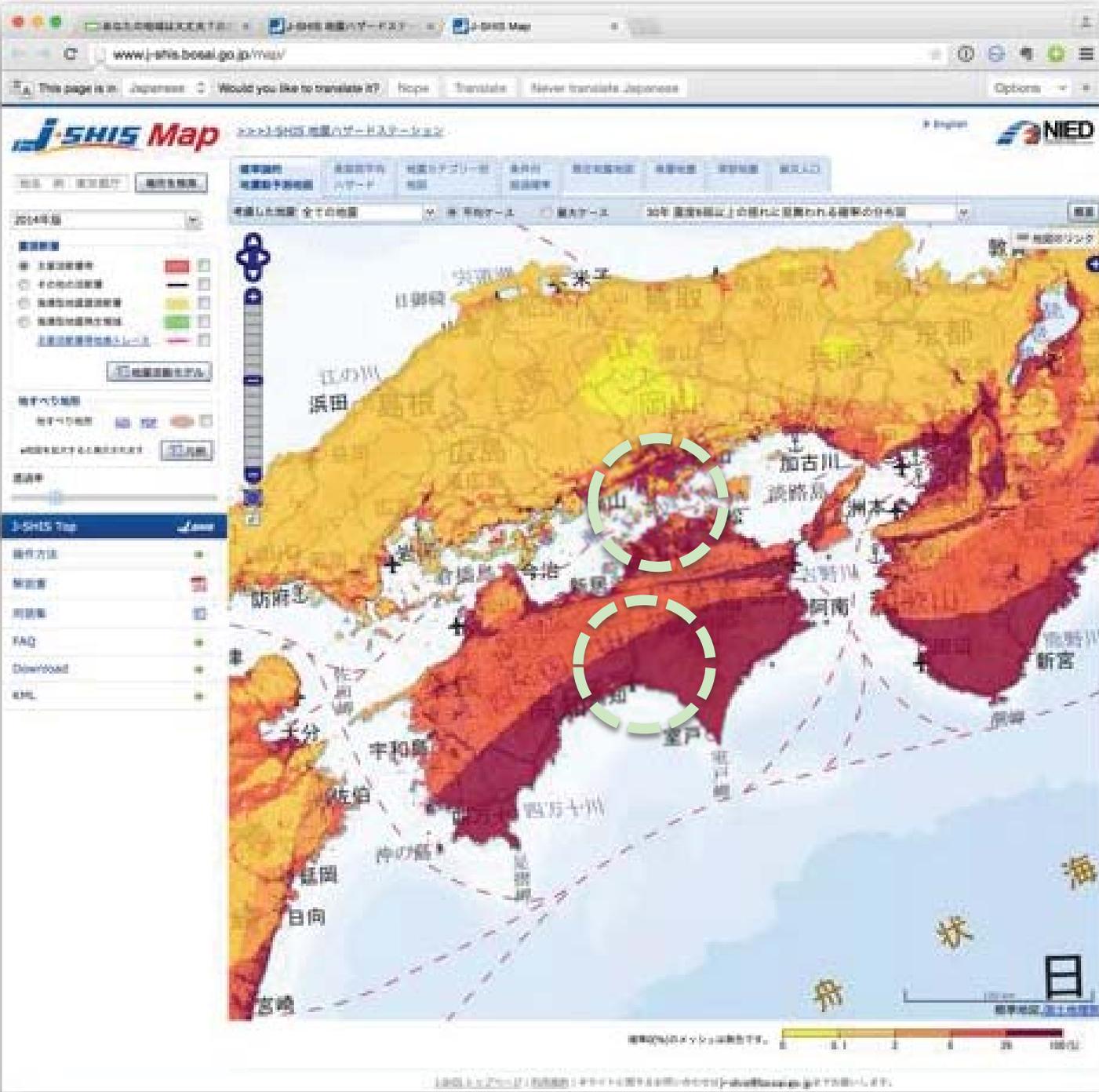
地震初期微動でのP波と呼ばれる小さな揺れ（縦波）と主要動でのS波と呼ばれる大きな揺れ（横波）が同時に発生 --> 到達時間が異なることを利用 <http://jutaku.homeskun.com/legacy/taishin/jisin/kinkyu.html> より引用

# 緊急速報から経路制御まで



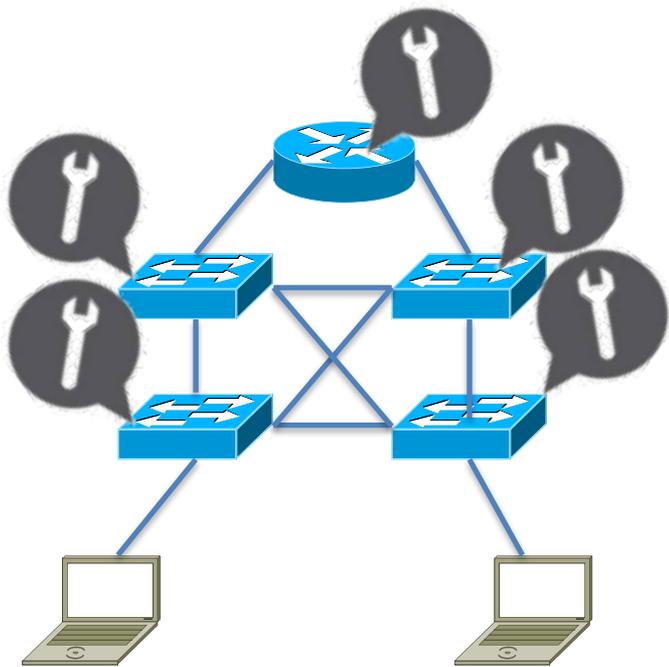
# 今回のシナリオ





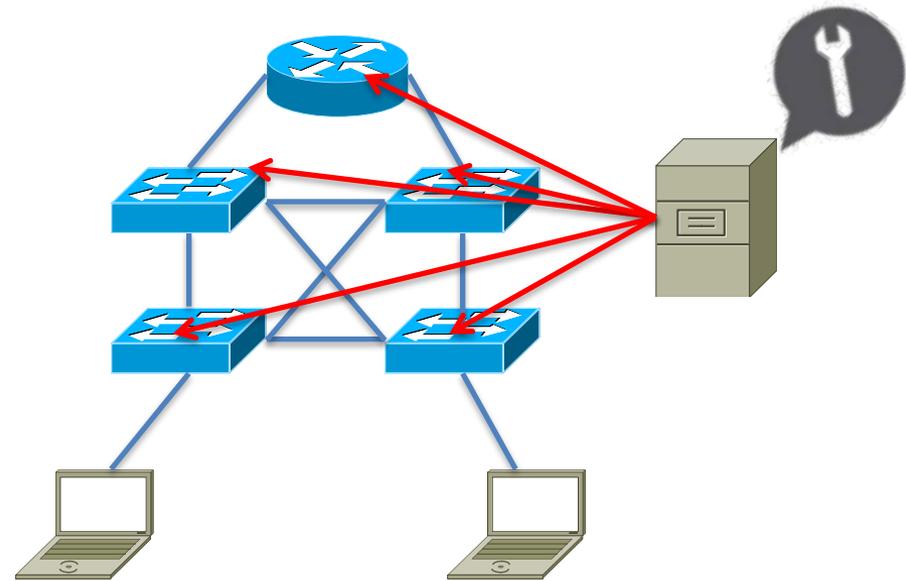
# Open Flowとは

## 従来のネットワーク

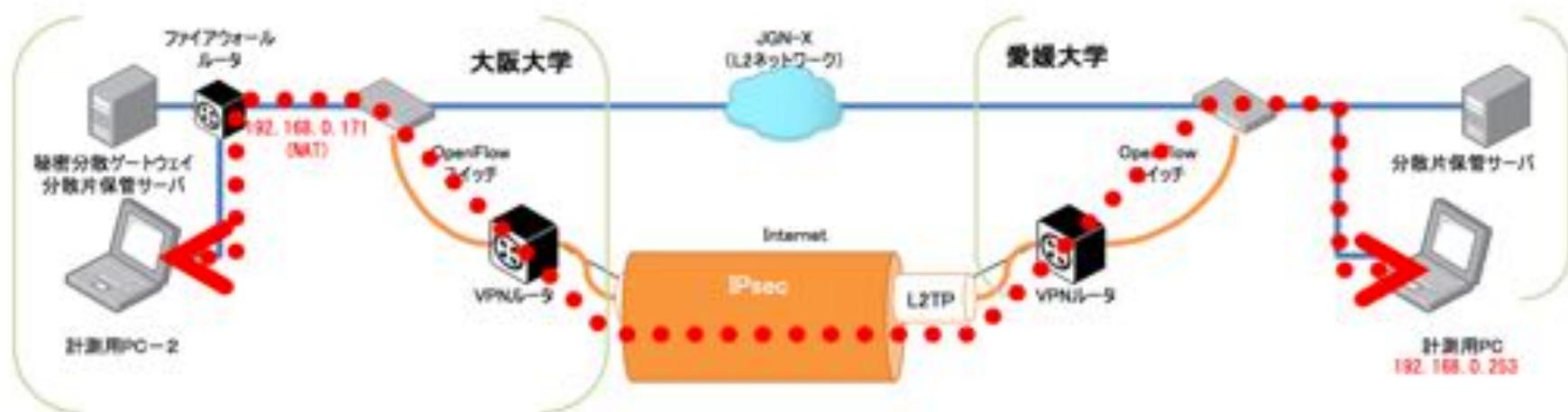
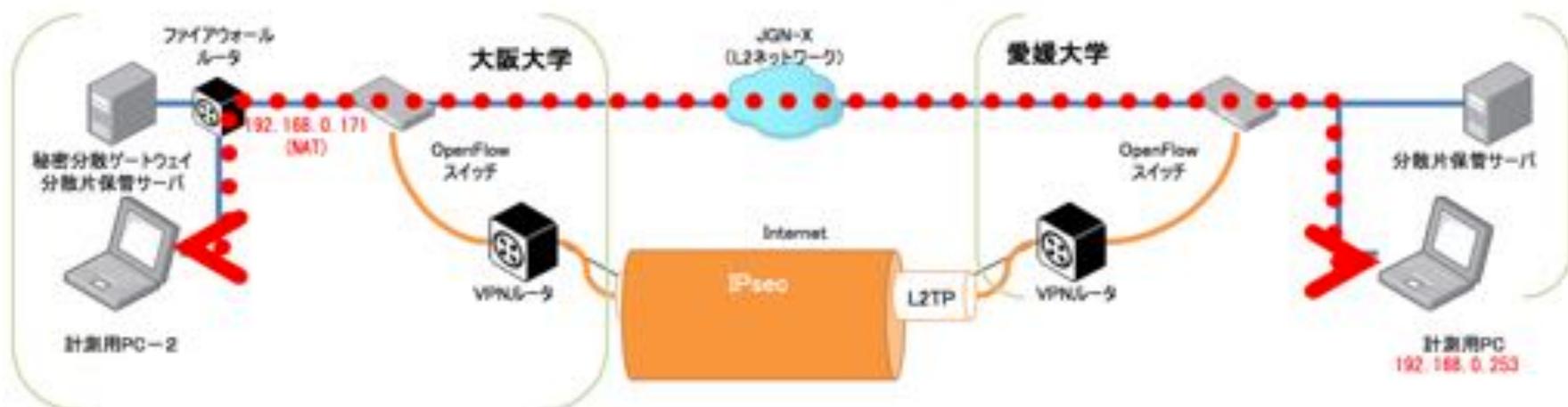


- ネットワーク機器が自律的に判断
- 正確かつ安定して稼働するのに多大な労力
- ちょっとしたことの変更が困難

## Open Flow ネットワーク



- 集中的に管理
- 挙動も整合性を取りやすい
- 多彩なポリシーに従った設定



# 結果

試験項目	使用回線	実施	protocol	送出レート	時間[秒]	データサイズ	送出パケット数	パケットロス数	パケットロス率	実行速度
通常時(帯域測定)	メイン回線	1回目	UDP	100Mbps	120	1470	1025470	1	0.0001%	-
	メイン回線	2回目	UDP	100Mbps	120	1470	1023522	0	0.0000%	-
	メイン回線	3回目	UDP	100Mbps	120	1460	1034044	1	0.0001%	-
	メイン回線	4回目	UDP	100Mbps	120	1460	3904515	1	0.0000%	-
通常時(帯域測定)	バックアップ回線	1回目	UDP	100Mbps	10	64	309711	255419	82.4701%	2.76M
	バックアップ回線	2回目	UDP	100Mbps	10	1460	86204	52238	60.5981%	37.6M
	バックアップ回線	3回目	UDP	100Mbps	10	1470	85467	51561	60.3285%	37.8M
	バックアップ回線	4回目	UDP	100Mbps	120	1470	1025073	622215	60.6996%	39.4M

試験項目	使用回線	実施	protocol	送出レート	時間[秒]	データサイズ	送出パケット数	パケットロス数	パケットロス率
バックアップ回線パケットロス測定	バックアップ回線	1回目	UDP	30Mbps	120	1470	306111	18	0.0059%
	バックアップ回線	2回目	UDP	30Mbps	120	1470	306072	27	0.0088%
	バックアップ回線	3回目	UDP	30Mbps	120	1470	305995	16	0.0052%

試験項目	使用回線	実施	protocol	送出レート	時間[秒]	データサイズ	送出パケット数	パケットロス数	パケットロス率
バックアップ回線パケットロス測定(再)	バックアップ回線	1回目	UDP	30Mbps	120	1470	306111	45	0.0147%
	バックアップ回線	2回目	UDP	30Mbps	120	1470	306072	16	0.0052%
	バックアップ回線	3回目	UDP	30Mbps	120	1470	306035	22	0.0072%

試験項目	使用回線	実施	protocol	送出レート	時間[秒]	データサイズ	送出パケット数	パケットロス数	パケットロス率
バックアップ回線パケットロス測定 (低速レートでの試験)	バックアップ回線	1回目	UDP	10Mbps	120	1470	102037	20	0.0196%
	バックアップ回線	2回目	UDP	10Mbps	120	1470	102037	7	0.0069%

試験項目	使用回線	実施	protocol	送出レート	時間[秒]	データサイズ	送出パケット数	パケットロス数	パケットロス率
連続切替試験 OFサーバーより連続切替試験	(切替)	-	UDP	30Mbps	2100	1470	5350801	15739	0.2941%

切替に0.29%程度の瞬断が見られる以外は  
通常通りの継続した通信を実現

# 今後の課題

- 緊急地震速報(演習)との連携
- 各経路の物理的位置情報(経度・緯度)と、被災予想地域を踏まえた経路の計算
- JGN-X/RISE Open Flowテストベッドネットワーク上での大規模な検証