組織間連携による
電子情報の遠隔バックアップの検討

西村 浩二
広島大学 情報メディア教育研究センター

「クラウドサービスのためのSINET&学認」説明会（広島会場）

本日のお話

- 西日本地区での取り組み
  - 学際大規模情報基盤共同利用・共同研究拠点 公募型共同研究（JHPCN）
    「電子情報の大学間相互保持に向けた遠隔バックアップ技術の研究」
- 組織間連携による分散ファイル管理システム

過去の報告
- 学術認証フェデレーション及びSINETサービス説明会（2009年12月4日）
- SINETの活用事例集（p.102）
  「キャンパスネットワーク（HINET2007）におけるWeb認証システムの構築・運用」
  - http://www.sinet.ad.jp/case/hiroshima
- SINET&学認説明会（2010年12月9日）
  「学認を利用したキャンパスネットワークの利用者認証」
  - http://www.sinet.ad.jp/inform/news-1/gj-kyoto.pdf
  - http://www.sinet.ad.jp/inform/news-1/gj-kyoto-d.pdf
- 学認活用事例集（ケーススタディ No.12）
  「ゲスト利用者のネットワーク認証に活用（広島大学）」
  - http://www.gakunin.jp/docs/files/12hiro.pdf

取り組みの経緯

- 7情報基盤系センター群
  - 北大、東北大、東大、名大、京大、阪大、九大
  - 重要な電子情報のバックアップを相互保持する仕組みを構築するための検討を開始
    - 規模が大きく異なる大学間でのバックアップの相互保持を検討
- 西日本地区大学情報関連センター長会議
  - 西日本地区電子情報統合バックアップ検討部会設置（平成21年12月）
  - 西日本地区電子情報統合バックアップシステム導入（平成21年度補正予算）
- 学際大規模情報基盤共同利用・共同研究拠点
  - 平成22年度公募型共同研究に九大地区から申請、採択された（課題番号：10-IS04）
  - 平成23年度も同様に申請し、採択された（課題番号：11-IS02）
    - 3/11 14:03に採択の連絡メール

共同研究体制（平成23年度）

西村　浩二	広島大学・情報メディア教育研究センター	研究の総括
天野　浩文	九州大学・情報基盤研究開発センター	ストレージ仮想化実験の計画と実施
岡村　耕二	九州大学・情報基盤研究開発センター	ネットワーク仮想化実験の計画と実施
赤井　光治	山口大学・情報機構メディア基盤センター	
林　豊洋	九州工業大学・情報科学センター	
大谷　誠	佐賀大学・総合情報基盤センター	
上繁　義史	長崎大学・情報メディア基盤センター	
柳生　大輔	長崎大学・情報メディア基盤センター	
永井　孝幸	熊本大学・総合情報基盤センター	大学保有電子情報の調査・分析、遠隔バックアップ実験
吉田　和幸	大分大学・総合情報処理センター	
青木　謙二	宮崎大学・情報戦略室	
下園　幸一	鹿児島大学・学術情報基盤センター	
舟木　慶一	琉球大学・総合情報処理センター	
橋本　忍	九州産業大学・総合情報基盤センター	
藤村　丞	福岡大学・総合情報処理センター	

取り組みの背景と目的

広島大学

大規模災害による情報損失に対する懸念

事業継続計画（BCP），継続的データ保護（CDP）

外部へのデータ預託に対する抵抗感

理解不足，セキュリティポリシー

遠隔バックアップ先確保のコスト

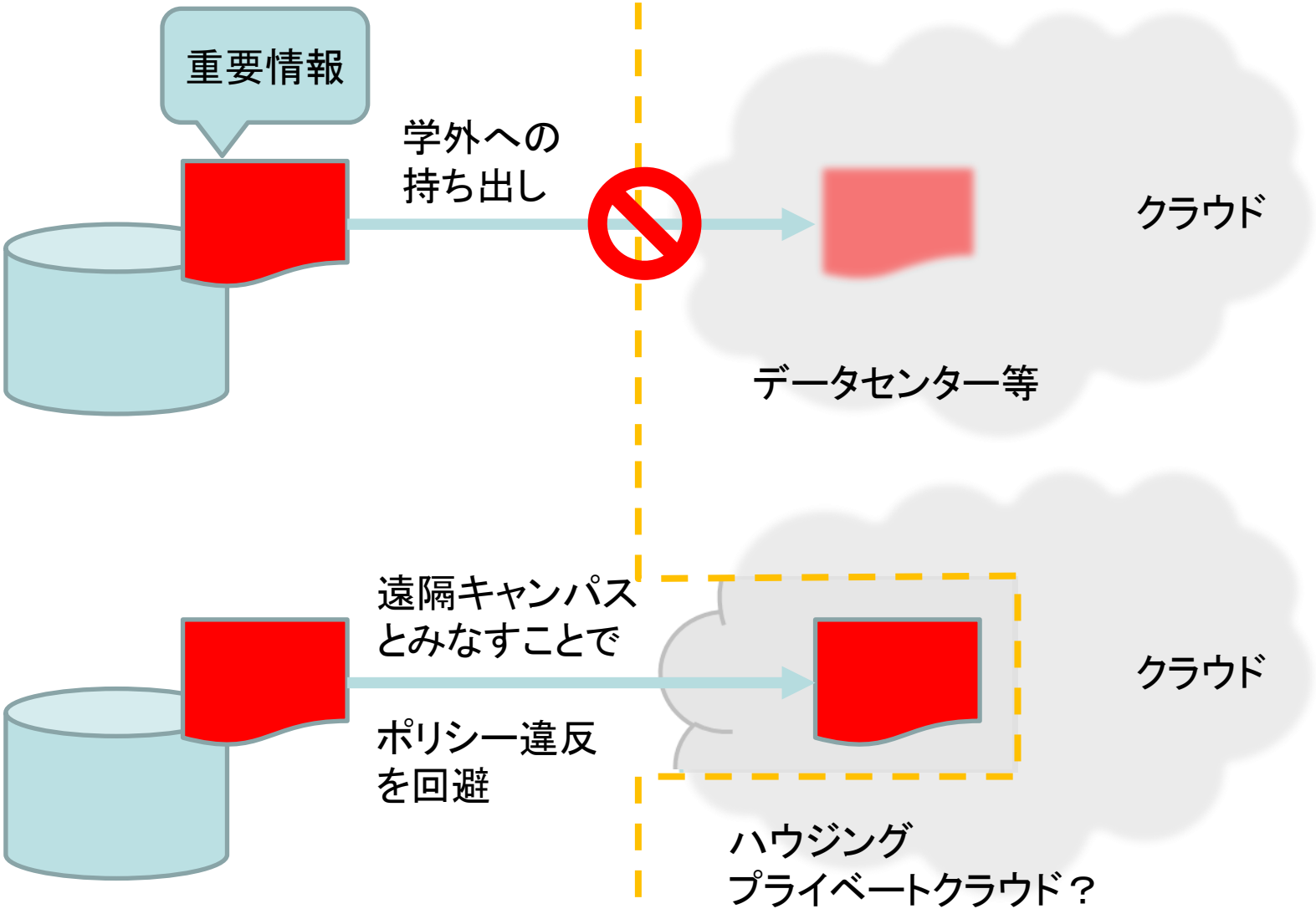
地理的分散度，余剰設備・人員

電子情報の安全な分散・相互保持による大規模災害対策

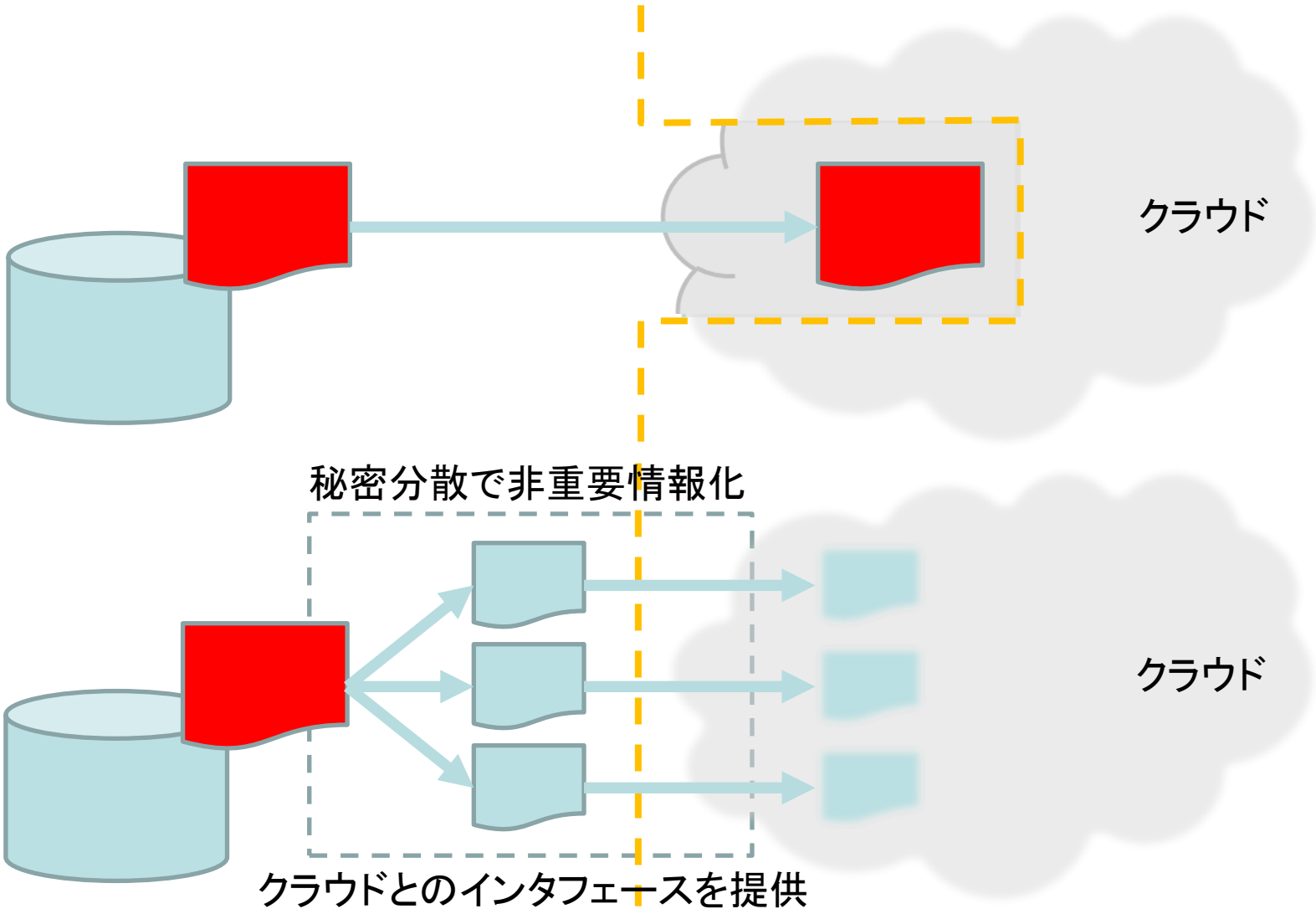
クラウド利用時の要検討事項

- セキュリティポリシーに違反しないこと
  - 重要情報の組織外への持ち出し禁止
    - 情報の分類
    - 「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」のクラウド対応
- 自組織以外の人に見られないこと
  - マルチテナントなクラウドサービスでのセキュリティ
  - 各状況（転送時、保存時、処理時）でのセキュリティ
- データがどこにあるかわかること
  - 国内？国外？データセンター？
  - ベンダーロックイン
- データを確実に消去できること
  - 破棄した情報が漏えいすることを防止するため、復元不可能な状態に（不可視化）する

現在の重要情報の学外への「持ち出し」



重要情報は非重要情報化して「持ち出す」



データがどこにあるかわかること

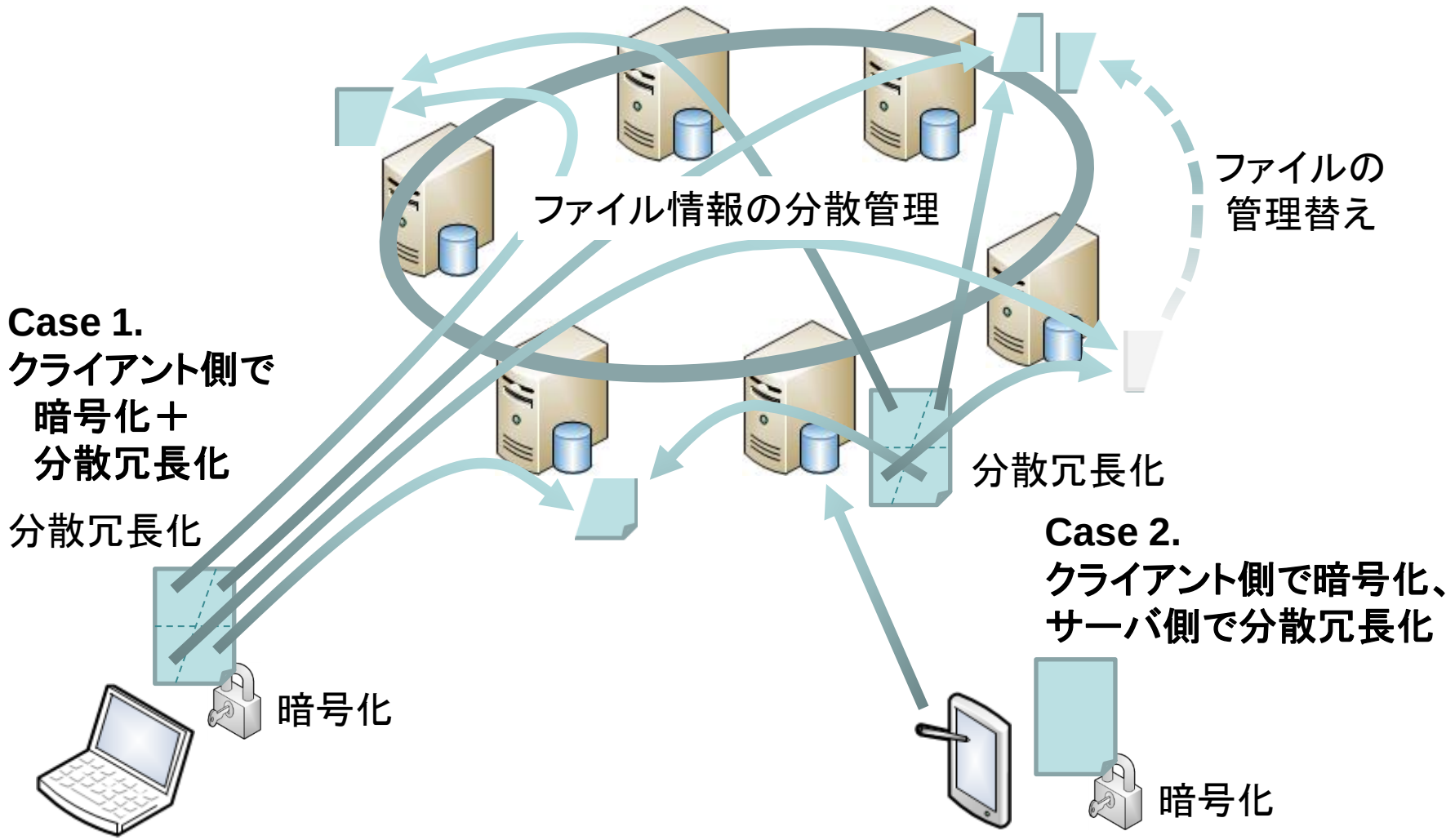
- クラウドの特徴（発想）とは正反対
  - 情報システム監査対策
    - データがどこにどのように保管されているか？
    - 商用クラウドサービスではデータのありかは一般に開示されない
      - 利用者が保管場所を管理できない
      - 消去されたことを確認できない
  - ベンダーロックイン防止
    - データの保管とサービス（処理）が一体となって提供されている
      - 他社のサービスを利用できない
      - データを簡単に取り出せない
- データとサービス（処理）の分離
  - データクラウド、ストレージクラウド
    - データのバックアップに特化したシステム
  - データとサービスのインタフェースを標準化
    - ローカルとクラウドのストレージ間をシームレスに（最終目標）

組織連携を前提とする場合の追加要件

- クラウド利用時の要検討事項
  - セキュリティポリシーに違反しないこと
  - 自組織以外の人に見られないこと
  - どのデータがどこにあるかわかること
  - 確実に消去できること
  - 構成変更に対する耐性（柔軟性）
    - ファイルサーバ管理者（複数）の権限を留保
      - 組織やファイルサーバ管理者の都合でシステムを止めたり、再構築したりできる
    - →利用者とファイルサーバ管理者のビューを分離
      - ファイル管理情報を分散・階層化

分散ファイル管理システム（DFMS）の概要

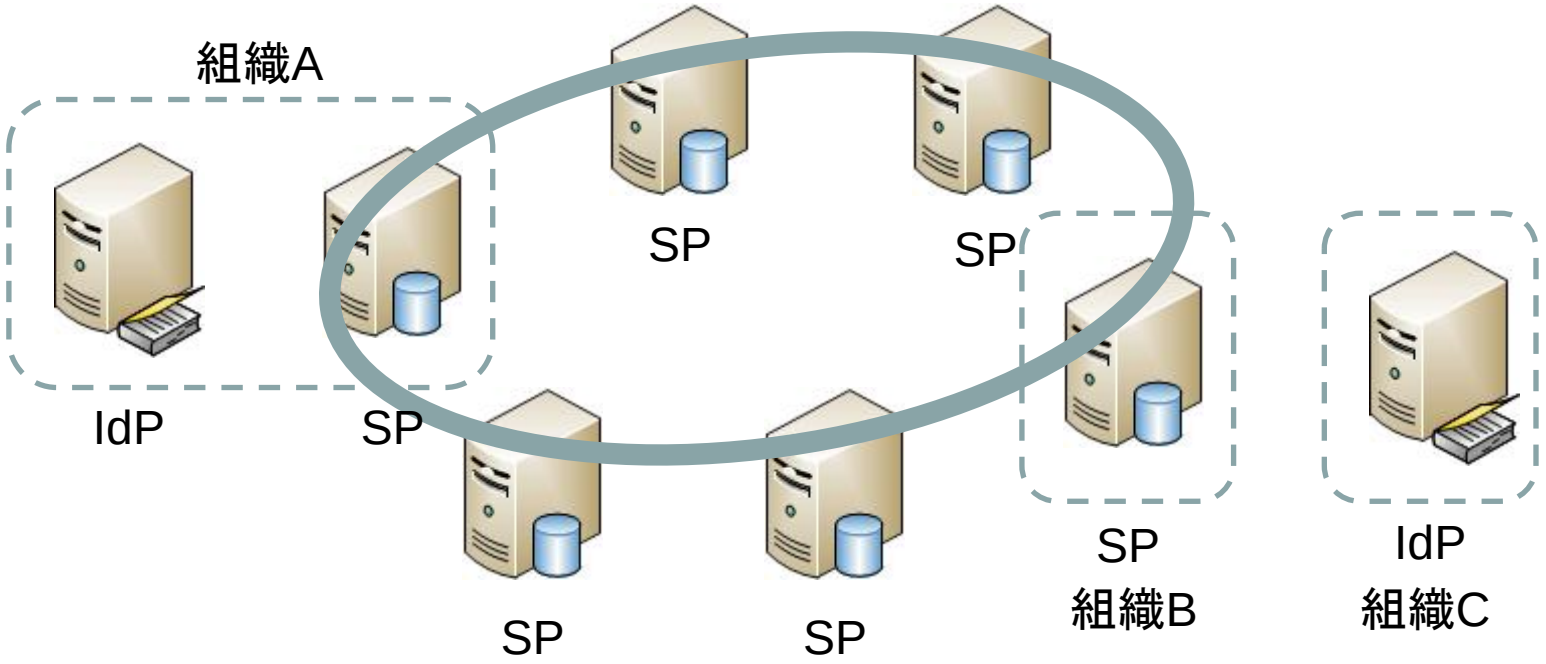
広島大学



サーバ群でSSOフェデレーションを構成

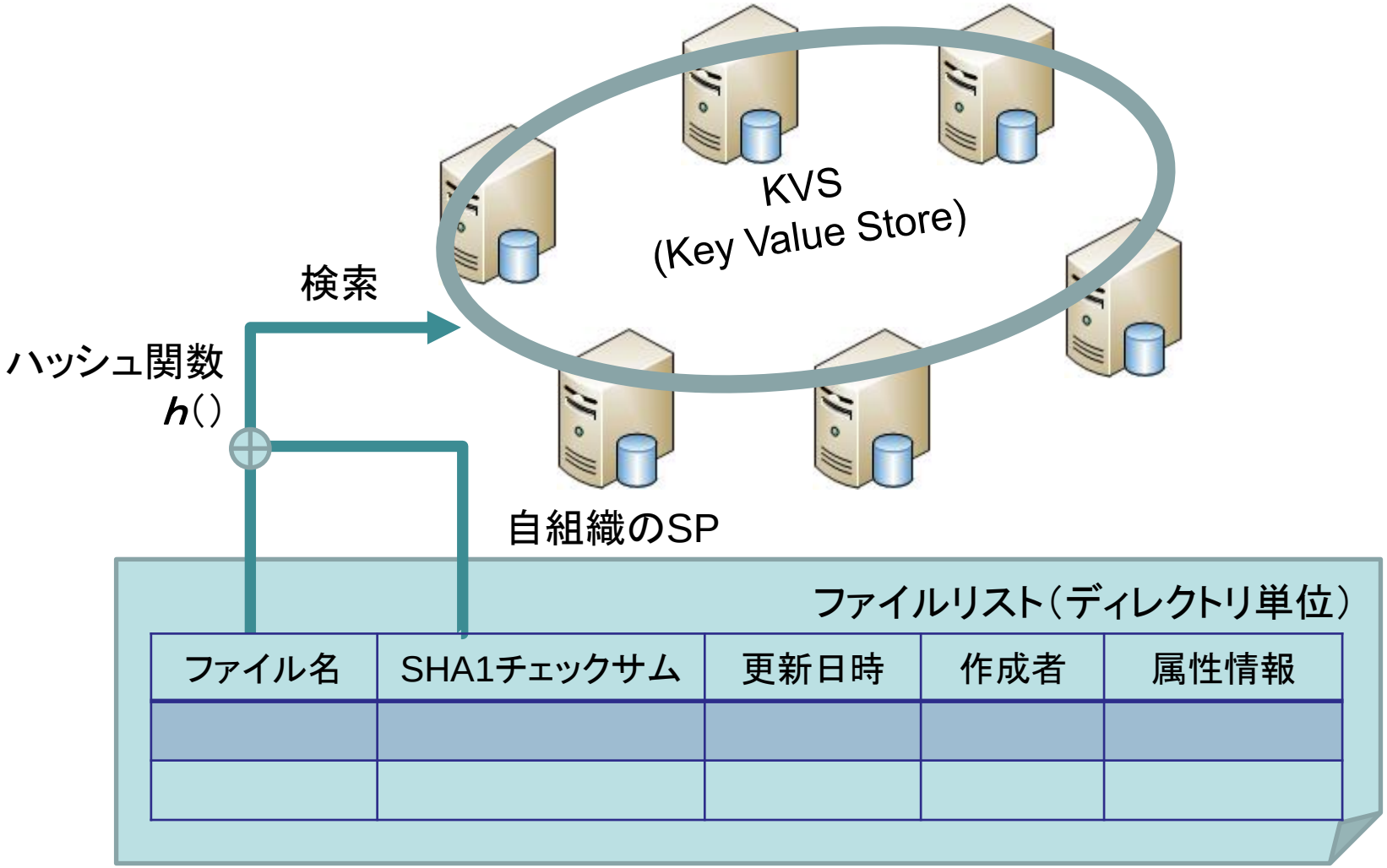
- フェデレーション（学認）への参加
  - フェデレーションへの参加時に審査を受け、他のIdPやSPと証明書を交換することで信頼関係を構築
- SP間の信頼関係を積極的に利用
  - 現在は主にIdPとSPの間の信頼関係に利用
  - 複数のSPでひとつの機能を実現する
- 利用者と管理者の権限を分離
  - IdP（認証）とSP（サービス）
  - サービス→管理データとデータ本体を分離
- 分散ファイル管理システム（DFMS）
  - （Case1）複数のSPは対等
  - （Case2）個々のSPはユーザのフロントエンドとして機能（FE-SP）し、（FE-SPを含む）他のSPがバックエンド（BE-SP）を構成する

サーバ群でSSOフェデレーションを構成 (Cont'd)

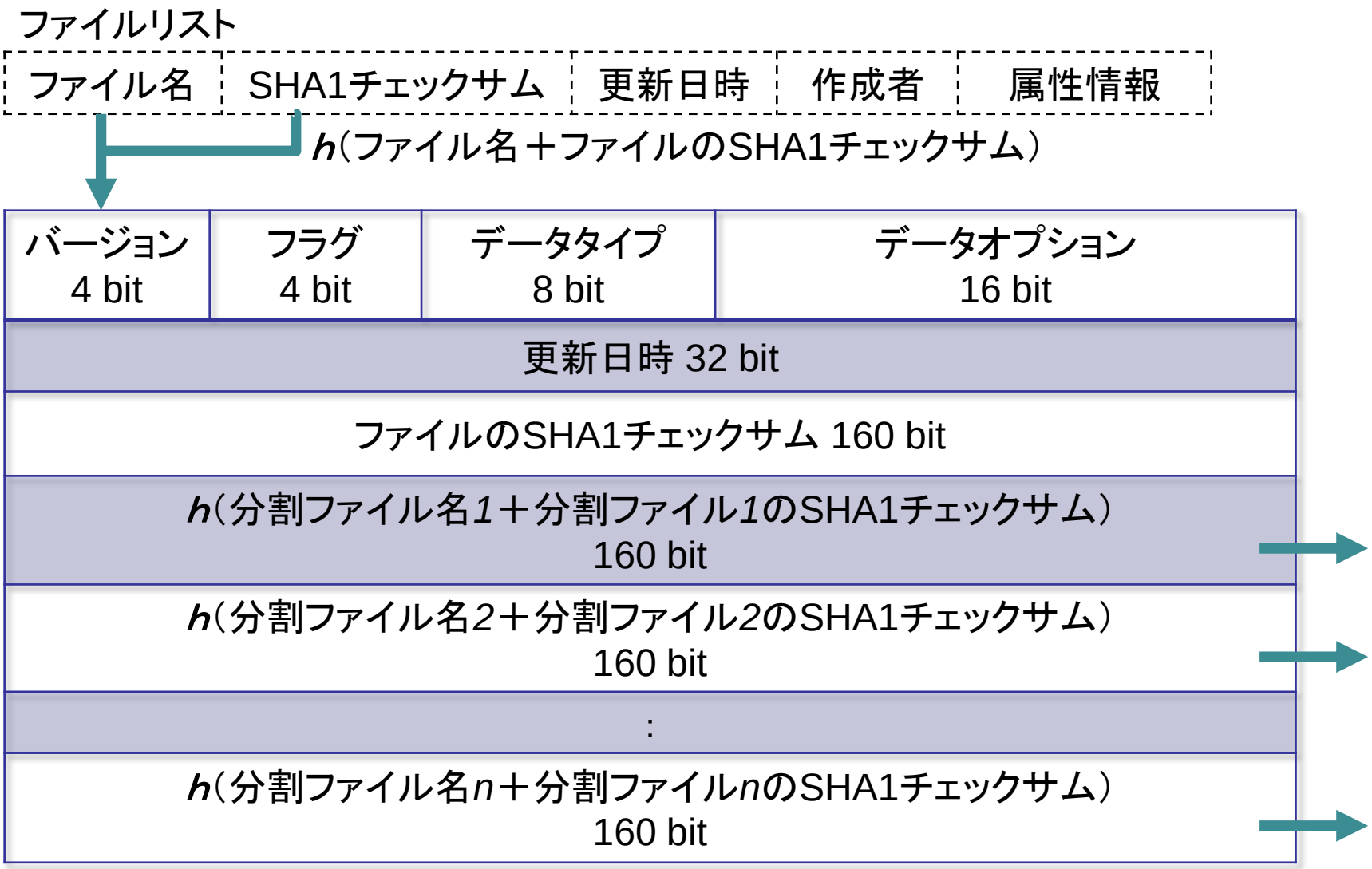


- IdPとSPの持ち方による違い
  - 組織A：IdPとSP…自前の設備で運用（大学等）
  - 組織B：SPのみ…ストレージのみを提供・管理（組織Cと契約）
  - 組織C：IdPのみ…利用者のみを提供・管理（組織Bと契約）
- 個人は組織Cと契約するとバックアップサービスが利用できる
  - 組織Bのように振舞う（SPを提供する）ことも可能

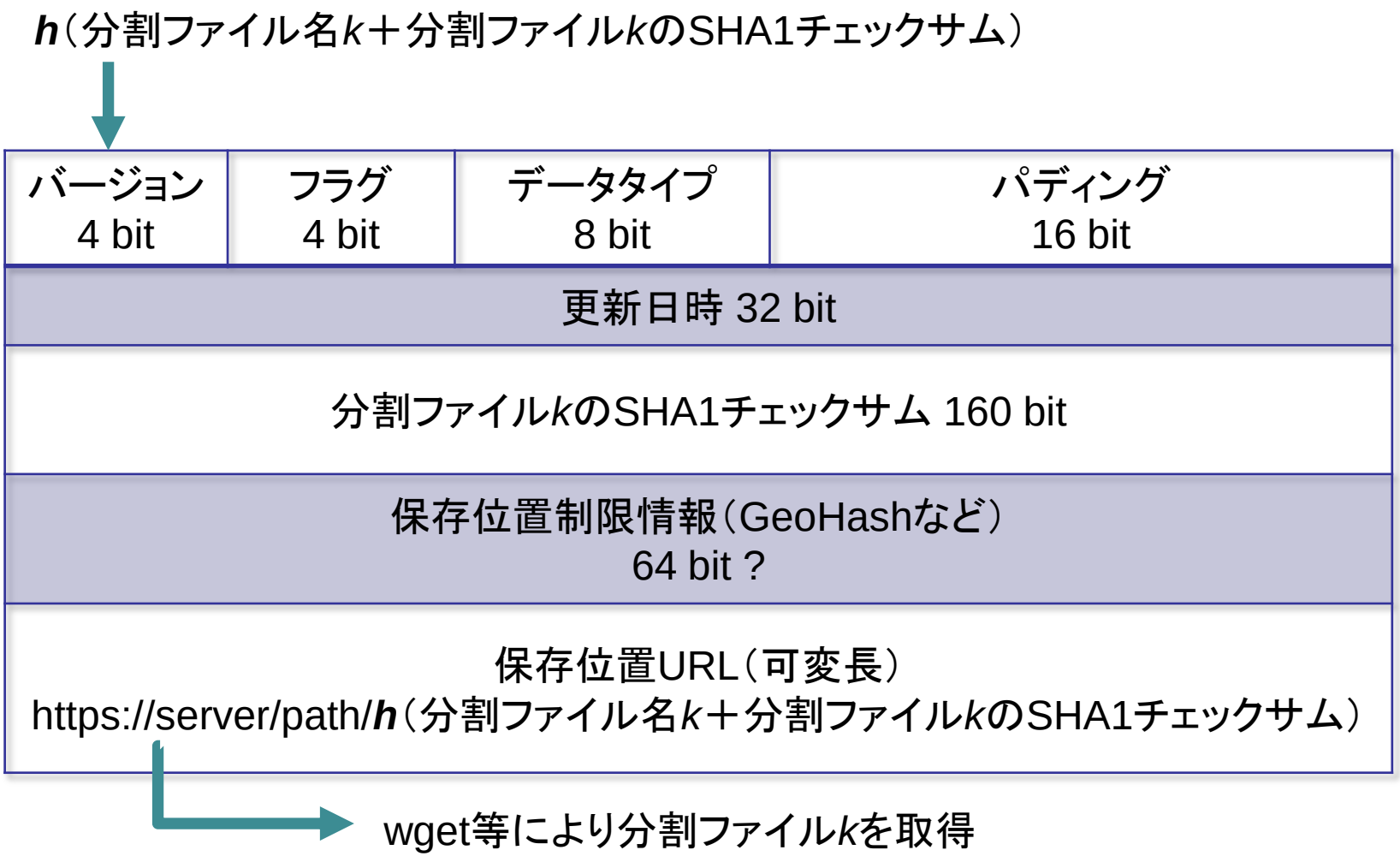
KVSによる分散ファイルの管理



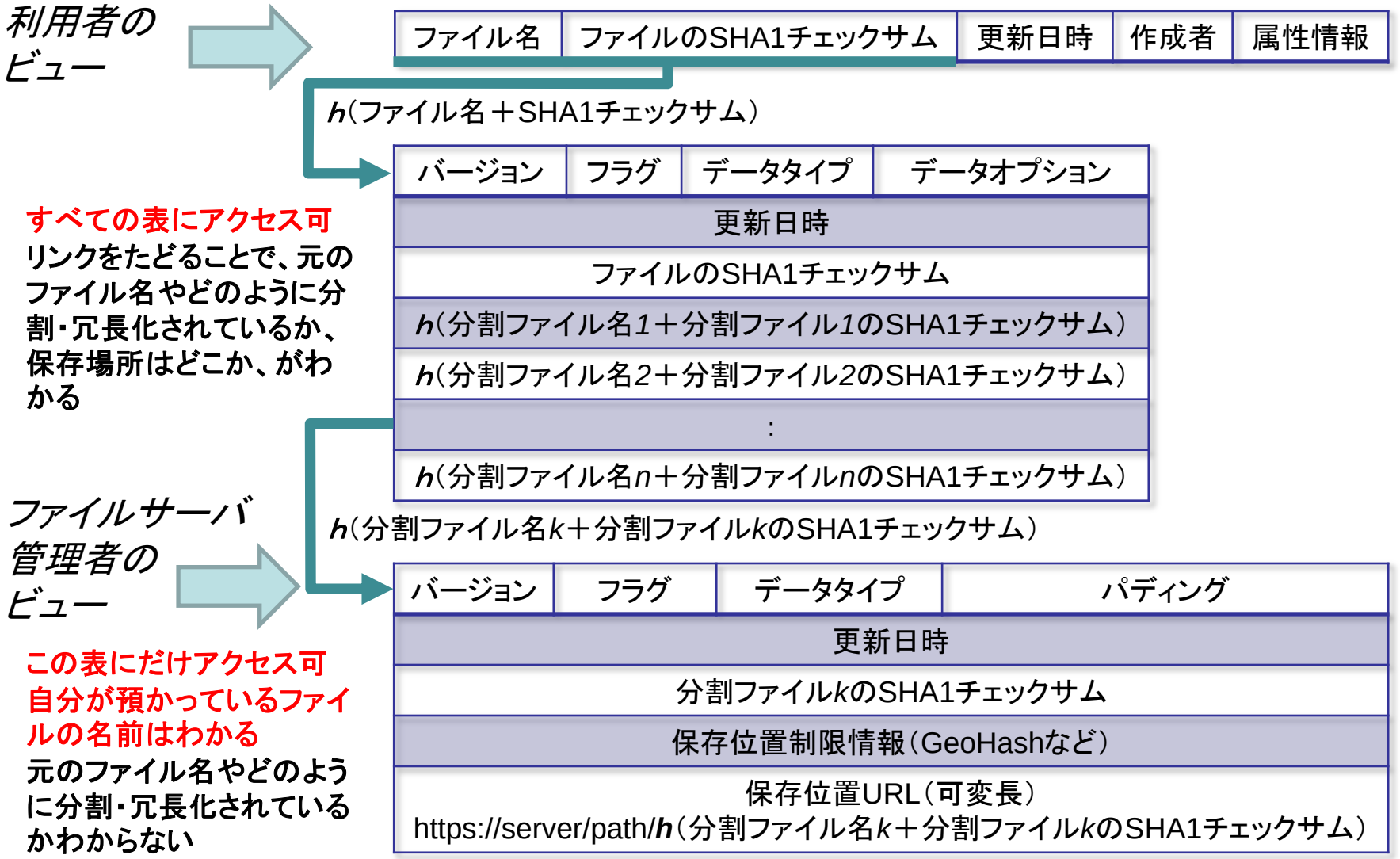
分割ファイル管理テーブル



保存位置管理テーブル


h（分割ファイル名*k*＋分割ファイル*k*のSHA1チェックサム）
バージョン
4 bit
フラグ
4 bit
データタイプ
8 bit
パディング
16 bit
更新日時 32 bit
分割ファイル*k*のSHA1チェックサム 160 bit
保存位置制限情報（GeoHashなど）
64 bit？
保存位置URL（可変長）
https://server/path/*h*（分割ファイル名*k*＋分割ファイル*k*のSHA1チェックサム）
wget等により分割ファイル*k*を取得

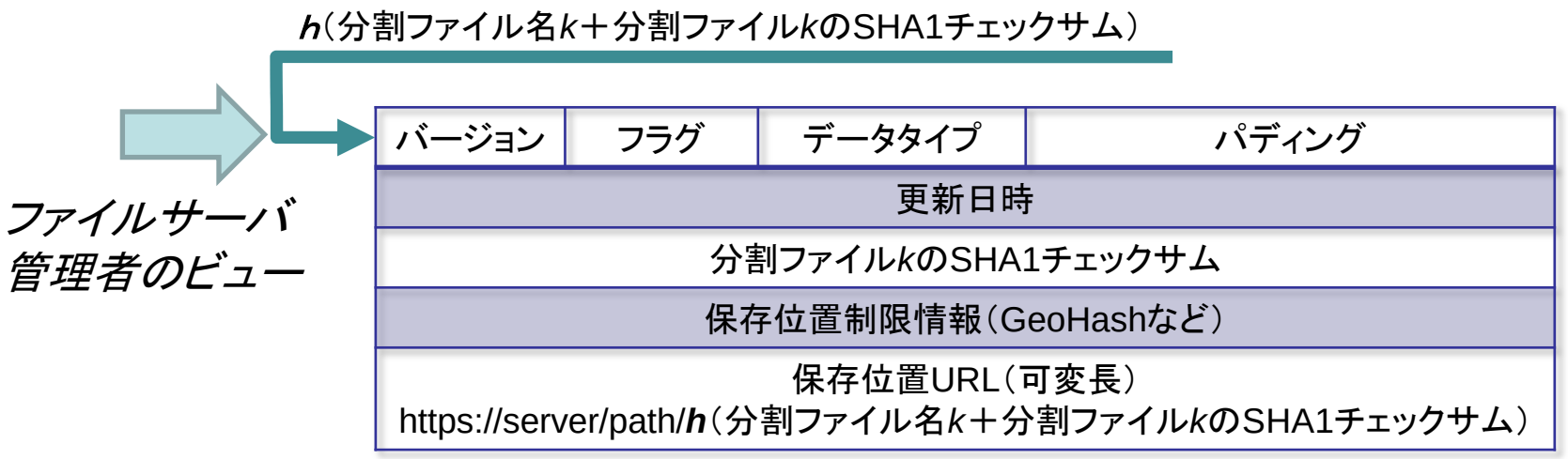
利用者とファイルサーバ管理者のビュー



- すべての表にアクセス可
- リンクをたどることで、元のファイル名やどのように分割・冗長化されているか、保存場所はどこか、がわかる

- この表にだけアクセス可
- 自分が預かっているファイルの名前はわかる
- 元のファイル名やどのように分割・冗長化されているかわからない

ファイルサーバ管理者の権限

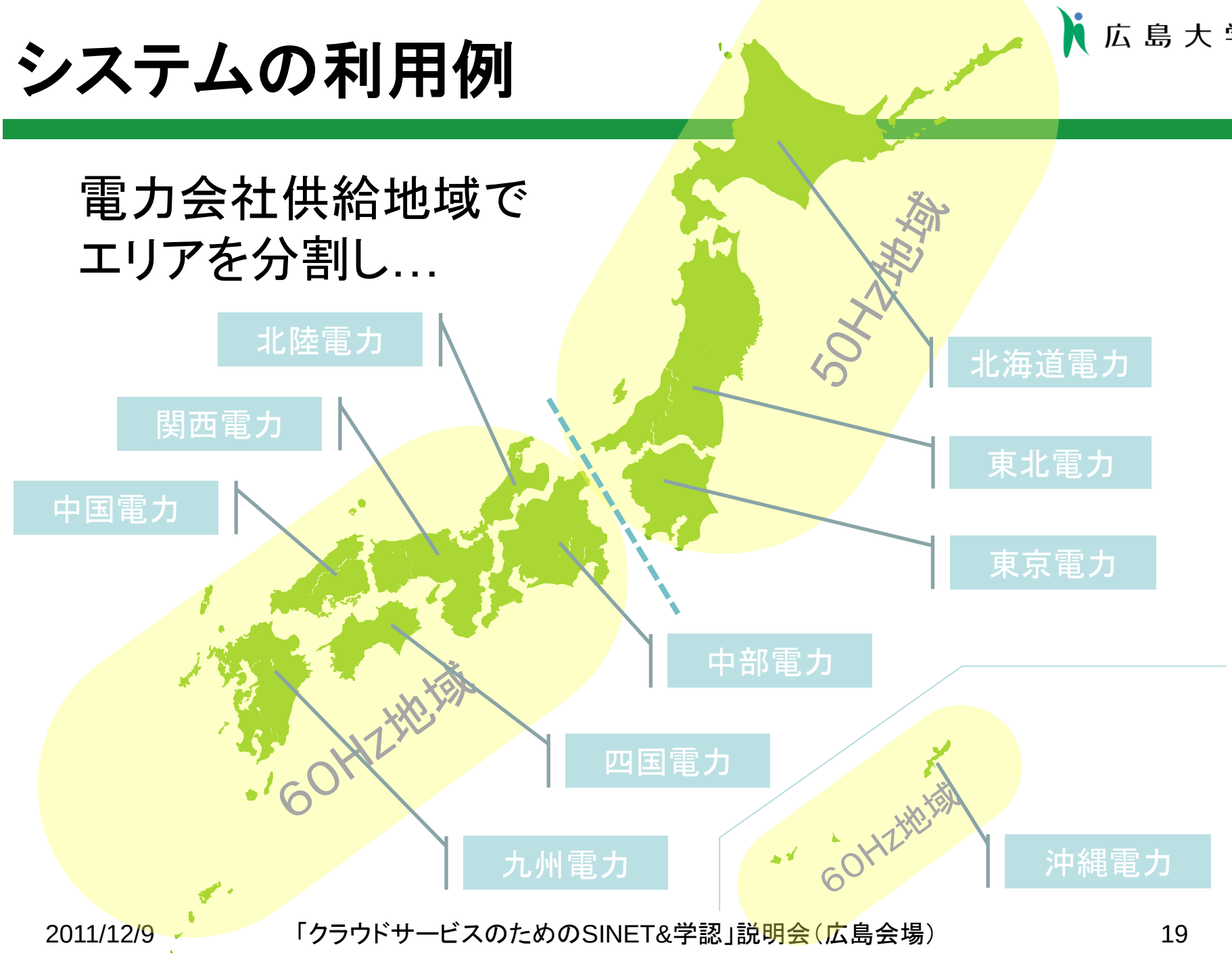


- 保存位置制限情報
  - GeoHashや緯度・経度などの地理情報を制限として含める
- 制限の範囲で、ファイルの再配置を可能とする
  - 同一グループ内（SPをグループ化している場合）
  - 同一エリア内（〇〇地方、都道府県）
- 分割ファイル管理テーブルを多段に適用することで再分割も可能
- （ファイルをすべて他のSPに移動すれば）SPをやめることも可能

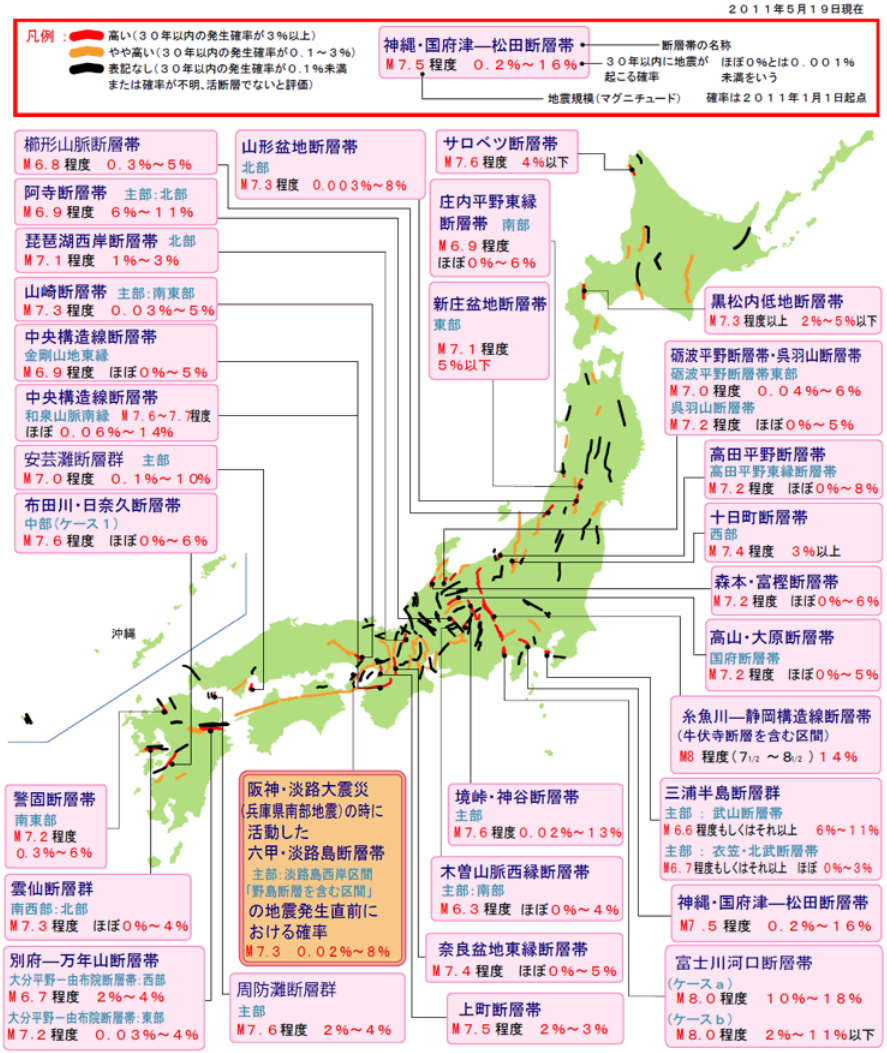
→ **いずれもファイルサーバ管理者の権限で実施できる**

システムの利用例

電力会社供給地域で
エリアを分割し…



活断層や海溝型地震の評価を加味すると…

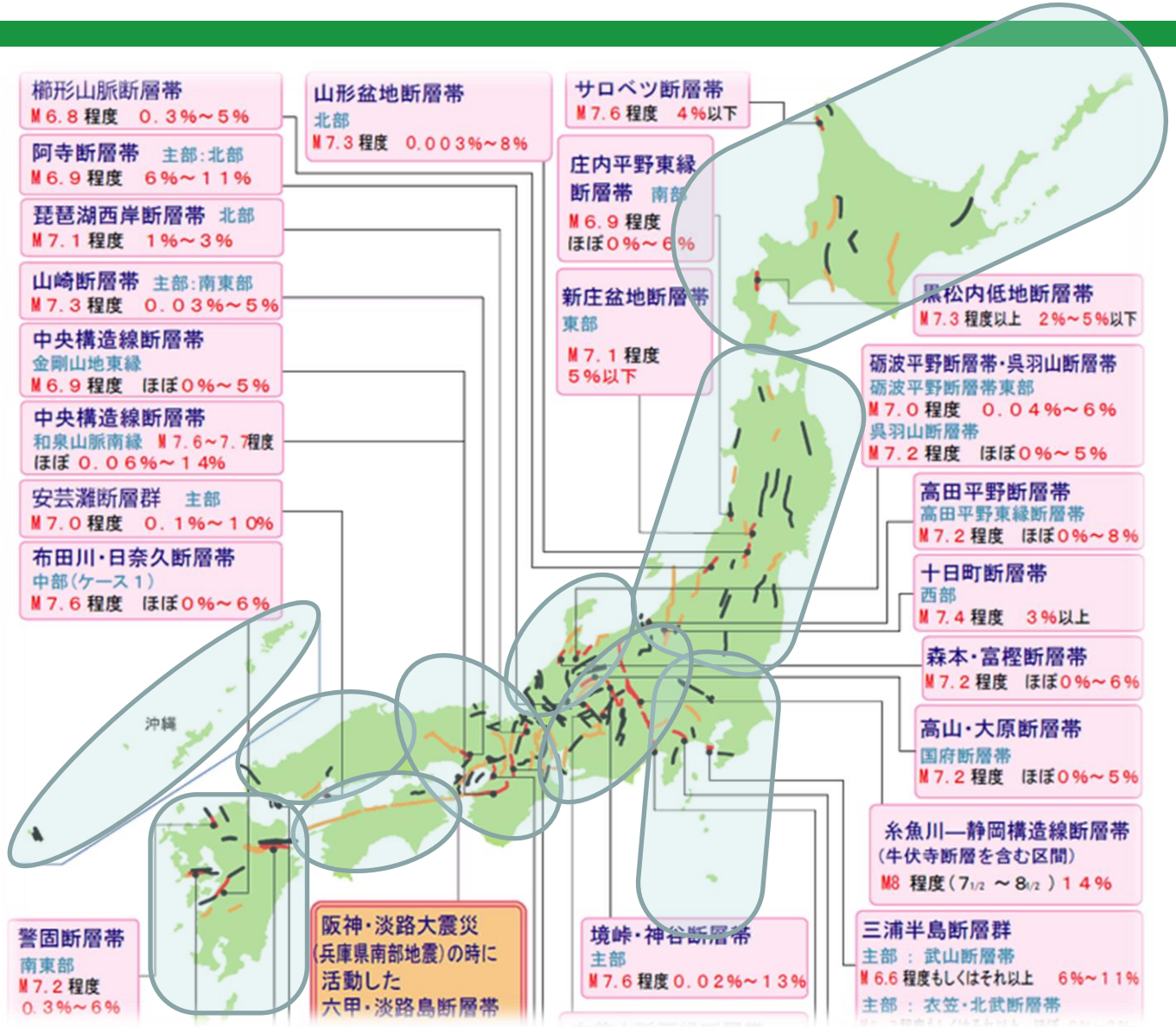


主要活断層の評価結果

主な海溝型地震の評価結果

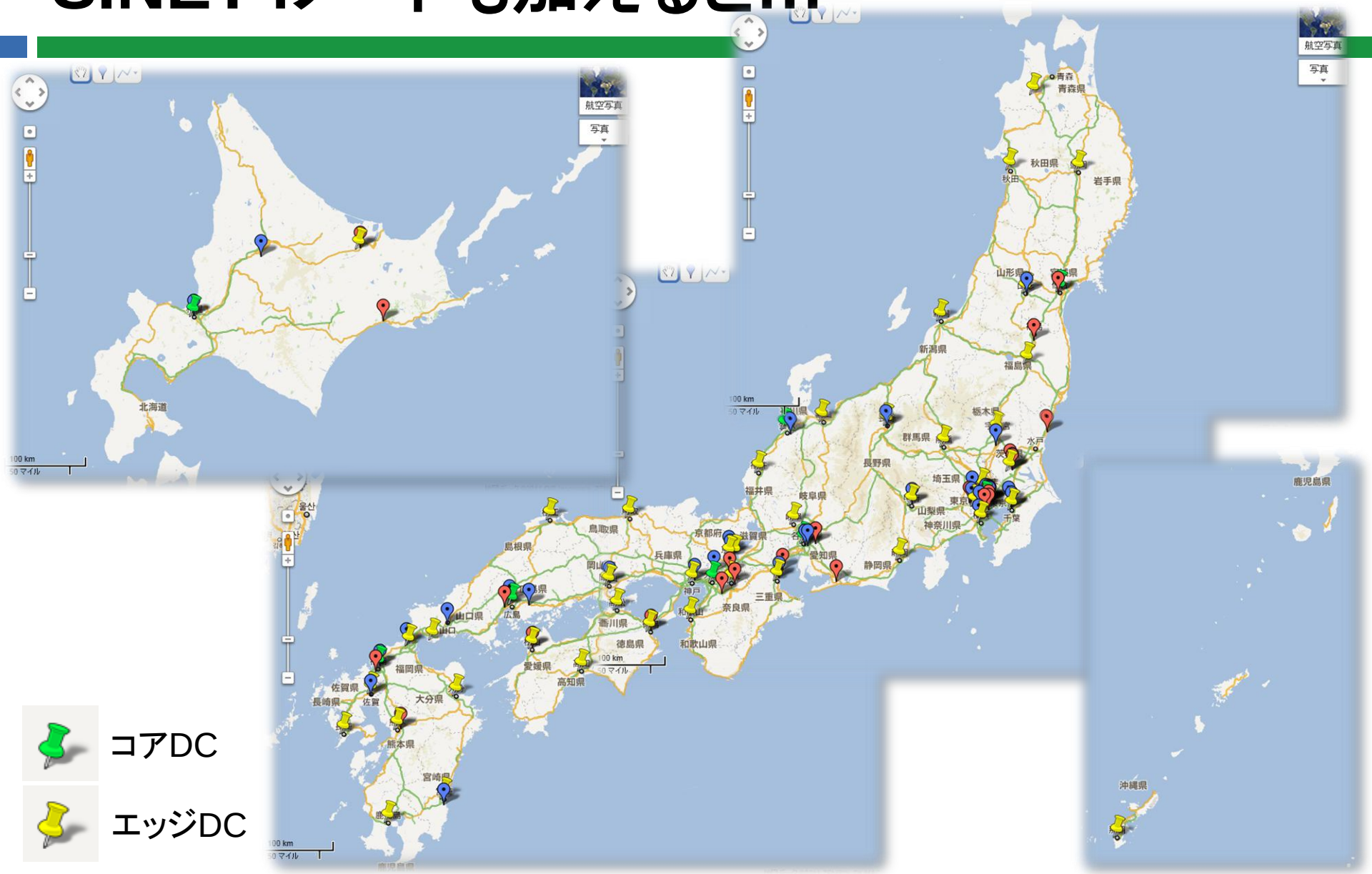
地震調査研究推進本部ホームページ
http://www.jishin.go.jp/main/p_hyoka02L.htm より

最適な配置が見えてくる…かも



学認参加組織（IdP設置場所）

SINET4ノードも加えると…



まとめ

- 西日本地区での取り組み
  - JHPCN研究課題（平成22, 23年度）
    - 「電子情報の大学間相互保持に向けた遠隔バックアップ技術の研究」
- 組織間連携による分散ファイル管理システム（DFMS）
  - 複数のファイルサーバ（SP）が連携してファイルを分散管理・保管
    - ファイルサーバ間でSSOフェデレーションを構成
    - KVSによる分散ファイル管理
  - 利用者のビューとファイルサーバ管理者のビュー
    - ファイルサーバ管理者に対してファイル情報を隠蔽
    - ファイルサーバ管理者としての権限（再配置・再分割）を留保
- 学認参加組織（運用・テストフェデレーション）の分布
  - SINET4ノード（DC）で補間すると全国をカバー可能