100年データストアの必要性とその構築・運用
100 Years Lasting Data Base

福原 英之[a], 佐分利 徹[a], 藤田 龍太郎[a], 宮崎 敏明[b],渡辺曜大[b],岩瀬 次郎[b],加羅淳[b], 林 隆史[b]

ネットワンシステムズ(株) [a] 会津大学[b],

Abstract データストアは、種々のシステムで重要な意味をしめている。2011年の震災と原発事故は、従来にも増して、長期にわたって利用可能なデータストアの必要性を示すこととなった。震災や原発事故に関連した健康調査のデータは、今後60年以上にわたり、保持、整備・運用することが必要である。また、震災時のＰＴＳＤ、アスベスト等の有害物質、放射線などについての影響については長期の追跡調査が必要である。これまでも、ライフコースデータや種々のの応疫学調査のデータ歴史的資料のデジタルアーカイブなど、長期にわたりデータを残さねばならないものは存在していたが、それらのシステムにおいて、社会制度、基本となるコンピュータ・ネットワーク技術の変化に対応できるようにするための取り組みは十分ではなかった。制度や技術の変化に対応したデータストアと関連システムを維持するためには、変化に対して柔軟に対応が可能な総合的な対応策が必要となる。例えば、２つののシステムが密結合すると、一方のシステムの変化に伴って他方のシステムも大きな影響をうけることになるため、２つのシステムは疎結合する必要がある。一方、各種のデータには入力ミスなどが避けられないと考えるべきだが、元データについては、各種測定の生データ同様、書き換えは好ましくない。修正であっても、修正前と修正後のデータを残すべきである。また、固定したスキーマでは、データへの要望の変化に対応するのは困難である。以上をふまえ、我々が今まですすめてきた、構造化オーバーレイ・ネットワークに関する研究の知見を活用したデータストアの構築・運用方法を提案する。

Keywords: データストア、メッセージング・ネットワーク、メッセージ・メディエーション、

はじめに

2011年の震災と原発事故は、情報システムやデータの運用方法についていくつかの課題をなげかけた。地震による被害や今後の防災に必要だと思われるデータ、放射線による健康などへの影響を確認するために必要なデータ、半減期が長い核種による放射線のモニタリングデータなどは、数十年から100年のオーダーで保存し、利用可能な状態にすることが必要となった。ディジタルデータは単独で存在しても利用できない。そのデータを管理し、利用者のアクセスを可能にするシステムがあってはじめてそのデータは利用可能になる。さらに、様々な制度、法律、権利等の許可する範囲でデータはアクセス可能であるし、制度が要求するデータアクセスは、システムが保証しなければならない。データアクセスには、利用者や利用端末・機器の認証が必要であり、利用者とデータ提供者との間の契約や法令に基づいた認可をシステムが実現することが必要となる。

先に挙げたデータだけではなく、各種センサーデータは、過去の履歴も含めて長期的に残すべき種類のものが存在するし、ライフコースデータやがん登録などのデータは、長期的に利用できることが必要である。

これまでの情報システムの歴史では、ごく一部の例外や特殊な用途のシステムを除くと、数十年単位でデータやサービスが利用可能になっているものはほとんど存在しない。たとえば、インターネットで利用される様々なプロトコルとそれを利用したソフトはこの40年間で多数作成されたが、長期間安定してメンテナンスされているものばかりではなく、様々なソフトやプロトコルが使われなくなっている。

先ほど挙げたデータのいくつかは、平常時にアクセス可能なだけではなく、災害発生時にも利用できることが要求される。先に挙げたデータだけではなく、住民の治療履歴や投薬履歴などは災害時にも必要である。つまり、従来考えられていないような長期的にわたって利用可能であり、かつ緊急時にも利用可能なデータストアと情報基盤の構築・運用が必要であるということである。

インターネットが登場してから40年あまりが経過し、制度も利用形態も技術も変化したため、変化に追随できなかったもの、メンテンスをするためのコストが確保できなかったものなどは、使われなくなったり不安定になってしまっている。そのため、Future Internetとそれに関連する研究が進められている[1,2]。

数十年以上持つシステムは、情報基盤も含めて、Future Internet などの成果などを用いることが合理的でると考える。しかしながら、震災と原発事故によって、様々な条件が満たされるのを待つことができなくなった。本研究では、100年持続するデータストアを構築・運営する方法、そしてその実現を助ける情報基盤について提案を行うものである。

Future Internetの取り組みの多くは、新しく構築するネットワークを従来のネットワーク上に構造化オーバーレイとして、新しい機能をもたせようとしている。構造化オーバーレイ・ネットワークの利用の拡大は、これまでのシンプルなネットワークと比して、多様な機能の実現を可能にした。機能の多様化と高性能化は、利用者の要求に応じたローカルな仕様や運用ポリシーの実現を可能にしている。本研究でベースとするメッセージング・ネットワークも構造化オーバーレイ・ネットワークとして既存のネットワーク(IPおよび非IP)上に構築することができる[10]。これによって、基盤技術の変化や災害時のネットワーク障害にも対応することが可能である。

メッセージング・ネットワーク

メッセージ・ネットワーキングは、メッセージの内容に応じた転送経路設定(content-based routing)、利用者(情報提供者も含む)の認証／認可／課金機能、転送されるメッセージの内容や形式の調整・変換(メディエーション)を主な機能として、情報伝達にかかわる処理をネットワーク・セントリックな方法で解決しよう

とするものである。ネットワーク・セントリックな手法では、メッセージの発信者及び受信者、メッセージの各項目とその内容、あらかじめネットワーク上に登録し適切なアクセス制御のもとに公開されたルールに基づいて、転送経路やメッセージに施す処理を選択する。メッセージの処理ルールの管理や処理そのものをネットワークへアウトソーシングすることにより、サービス提供者もサービス利用者もリストの管理コストが減少し、より自由にサービス提供やサービス利用をすることができるようになる。同じサービスを提供できるサービス提供者やサーバが複数存在する場合、ネットワークやサービス提供者の負荷に応じて、適切なパスを選択して、より早く処理結果をサービス利用者に提供することが可能となる。

この考えに基づいて構築されるネットワークをメッセージング・ネットワークと呼び、エンドポイント間のメッセージのやりとりをメッセージングと呼ぶ[10]。SOAP/XMLやCORBAによるモジュール間データ交換などもメッセージングである。メッセージング・ネットワークを構築してメッセージ・ネットワーキングを実現する方法はいくつか考えられるが、我々は現時点で利用可能であり、既存システムに与える影響がほとんどない方法として、構造化オーバーレイ・ネットワークを用いた手法を中心に検討してきた。メッセージング・ネットワークは、OSIネットワークモデルにおけるLayer 3ネットワーク上にLayer 7ネットワークとして構造化オーバーレイの型式で構築され。Layer3とLayer7でのサービスを共存して提供することが可能である[10]。メッセージ・メディエーションと呼ぶ機能によって、メッセージ送受信者間のメッセージの項目の調整や変換を実現できる。メッセージ・ヒストリは、メッセージング・ネットワークにおけるメッセージに関する種々の処理、処理前後のメッセージの記録から構成され、伝送されたメッセージそのものに加え、メッセージの提供者、利用者、メッセージに施された処理、関連する業務などが時系列で記録される。様々なポリシーに対応する仕組みとして、オーバーレイ・ネットワークに複数のスライスを作成す方法が提案されている[20]が、メッセージ・メディエーションを用いることで、ポリシーによってスライスされたオーバーレイ・ネットワーク間をポリシー調節しながら連携させることが可能である。

ネットワークセントリック手法による情報基盤

サービス、コンテンツ、データは、ダイナミックな連携によって、その相乗効果が期待される一方、同一サービス、コンテンツ、データであっても、その形式や利用ポリシーが、提供者や利用者、利用目的によってそれらの属性が異なる可能性がある。これらの属性の異なるものを連携するためには、最低限の標準化やとりきめが必要である。しかしながら、各種の情報について細部まで標準化をしようとすると、時間もコストも膨大になる可能性がある。アプリケーション・インタフェースやデータフォーマット、認証・認可ルールなどについての最低限の標準化とSLA実施のための必要最低限の法制度を整備した上で、残った差異は、システムによって、変換するのが合理的である。サービスやデータの流通のための「疎結合」を実現する手段は、サービス提供者やサービス利用者が用意するのではなく、ネットワーク上に情報基盤の機能として（ネットワークセントリックに）提供するのが、管理コストやスケーラビリティ、事業継続性の観点から合理的であると考える[6-8]。提案情報基盤では、情報消費者が必要とする情報を、情報基盤上の機器群が自律的に形成した最適なパスを介し、適切な処理を施した上で届ける。情報提供者は、情報利用者が必要とすると予想される情報を用意しておき、前述の方法で情報が利用されたときに、その利用に応じて得られた対価を情報提供者と情報基盤運営者等で分配するようなモデルを想定している[8,10-18]。

セキュア・データストアグリッド

メッセージング・ネットワークを用いて、種々のデータストアを疎結合連携することができる[16]。提案データストアは、複数のデータストアを用いる。それぞれの用途や役割に応じて、Read Optimized Data Store, Write Optimized Data Store, Distributed Data Store などを用いてそれらをメッセージング・ネットワークを用いて疎結合連携する。また可用性、完全性、機密性を確保・高めるために、秘密分散法を用いる。この場合、データストアの分散数 M に対して複合に用いるデータストアの数 N は、M>N>1 となるようにする。こうすることで、一部のデータストアが災害などで利用できなくなったり、人為的に破壊されるようなことになっても、データの可用性と完全性を保つことができる。また、N>1 とすることで、機密性を高めることができる。さらに、データストアから送られてくるデータ（メッセージ）をデータの内容に応じて複数の経路に同時に routing (content-aware-routing) した上で、多数決によって、データの可用性、完全性を高めることも可能である。データストアは、必要に応じて多段にわけることもできる。元データを一次データストアグリッドに格納し、特定目的用に前処理したデータを2次データストアグリッドに格納することもできる。そうすることで、源データが保存されている一次データストアへの不要なアクセスを抑えることができる。また、目的が異なるユーザのアクセスを分離することができる。

本論文で論じているようなデータストアでは、100年程度、データを利用可能にしておくことが必要である。その間には、データ格納、アクセス技術や関連する制度が変わることを想定しておかねばならない。提案手法では、データの変換などをメッセージ・メディエーションで実現可能である。健康調査データでは、実験データ、観測データと同様にデータに誤りがあった場合に、元データを消去して訂正することは避けなければならない。元のデータに対しては、誤りがあったこと、その誤りの内容、誤りの訂正方法と訂正データのありかをリンクして、訂正データをつくることが必要となる。データの訂正などの記録は、メッセージング・ネットワークのメッセージングヒストリなどで残すことができる。また、key-value data store を使うことで、誤りデータを消すことなく、訂正データの追加が可能である。Key-value data store 自身の機能は全般にシンプルなものが多いが、提案手法による疎結合連携で、機能を付加することができる[12]。

情報の劣化・欠落防止

長期にわたってデータを利用可能にするためには、元データの持つ情報が失われたり改変されたりしないようにすることが必要である。そのために、我々は、メッセージングネットワークと、セキュアデータストアを用いた情報基盤構築を提案する。全てのデータについて、修正などにおいても、データは削除しない。データを修正する際には、データの修正の際には、データを修正したという記録と、修正前データから修正後のデータにリンクをはり、誤った修正や過剰な修正によって情報が欠損すること防

ぐ。データやデータ処理の記録にはタイムスタンプをつける。さらに、これらのタイムスタンプが期限や利用する暗号の危殆化によって失効する際には、メッセージング・ネットワークのメディエーション機能などを用いて、タイムスタンプを追加発行する。この際も元データは消さない。

これらの技術的枠組みに加えて、データの真正性を保証するための制度や、データアクセスの権限に関する法令、データ処理の記録に関する法令などの整備が必要となる。

災害などの緊急時にもデータを利用可能にするためには、前述の秘密分散や多数経路を利用したデータ伝送、非IP上の仮想ネットワークなども利用することができる。

アクセス制御

データストアの目的ごとにアクセス制御を適切に行うことが必要である。本論文で取り挙げているデータの多くは、個人情報が関係する。個人情報については、OECD8原則、すなわち、(1) 収集制限の原則、(2) データ内容の原則 、(3) 目的明確化の原則、(4) 利用制限の原則、(5) 安全保護の原則、(6) 公開の原則、(7) 個人参加の原則、(8) 責任の原則の要請を実現できるように、技術・制度の両面から対応するべきである。これらを長期間にわたって対応するためには、技術的、制度的両面からのしっかりした対応が必要であると考える。情報主体への情報開示には適切なアクセス制御が必要となる。広範囲で集めた情報に対して、情報主体が誰であるかを正確に特定するために、情報主体が転居しても追跡可能にしておく必要がある。マイナンバーなどの制度、技術的仕組みなどとの連動が、現在のところの合理的な実現方法であると考える。一方、情報主体へどのように情報を提供するかも重要である。情報主体の情報をもれなく提示する仕組みが必要である。単に現時点での情報だけではなく、修正、変更の履歴を提示できなれければ、管理している情報の信憑性に問題が生じる危険性がある。

疎結合連携

時間の経過とともに、制度や技術は変化する。その変化に対応していくためには、特定のシステム、基盤、サービスに依存しているのは好ましくない。データストアと関連するシステムやサービス、コンテンツなどを疎結合で連携するのが合理的である。提案手法では、データのやりとり、やその処理はネットワークを介したサービスで行うことを前提とする。サービスに対応していないアプリケーションなどについては、入出力や管理をサービス化する処理とその処理を行うノードを用意して対応する。仮想サーバ群におけるマルチテナンシーの実現: あるユーザのある処理を行うときには、その処理の種類と利用者が誰であるかに応じて、content-aware routing を行う。つまり、データの中身を利用者に応じて、どのサーバを利用するかを決定し、そのサーバに対して、必要とされるデータ変換や認証・認可作業を行ってデータを送り、その処理結果を利用者に送る。利用者へのデータ転送においても、必要なデータ変換を行う。提案手法では比較的小さい粒度のサービスを疎結合して、より複雑なサービスを実現する。個々のサービスの粒度を細かくすることで、各サービス間の依存性を低減することができる。サービス間の疎結合は、メッセージング・ネットワークのmessage mediation によって、データフォーマットやinterface protocol などの調整を行う。メッセージング・ネットワークにおけるcontent-aware routing によって、サービスを実行するノードを選択する。従来のネットワークのrouterが、より高速にデータを転送できるように負荷が少ないネットワークを選んでデータ転送を行うように、content-aware routerによって、処理能力が十分ある計算機にデータを送り、処理を行う。

グリッドサーバにおけるマルチテナンシー: サーバリソース群をグリッド上で実現し、処理を要求するノードと処理を実行するノードを分離する。さらに、グリッド上で処理を実行するノードを動的に入れ替え可能にしておく。Content-aware routingによって、利用者や処理内容に最適な実行ノードを選択しデータを転送する。

サーバリソース群の管理: サーバリソース群を実現しているグリッドに対して要求する処理は粒度の細かいプライオリティー付けを行う。要求されている処理のプライオリティーや、リソースの属性および稼働状況から、適切な頻度でリソースの動的管理を行う。また、リソースの利用状況をregistry を介して、メッセージング・ネットワークに伝えて、適切なrouting とそれによる計算機の稼働率向上を図る。マルチテナンシーとプライオリティー管理によって、サーバリソース群が常に高稼働率となるように全体のリソースを動的に最適化する。

Heterogeneous SOAとその疎結合・広域連携: メッセージング・ネットワークのMessage-mediation とcontent-aware routingなどの機能を用いた「アダプタ」によって、異種サービスの疎結合連携を可能にし、ベンダやプロバイダに縛られないheterogeneous SOAを実現する。個々の処理サービスを交換可能なユニットとすることで、災害時を含めたシステムの柔軟性と運用ポリシーのサステナビリティを高める。同時に、遠隔地を含めた広域連携を可能とすることによって、災害・事故時の事業継続性を高めることができる。ネットワーク的に遠隔の地点間の連携では、レイテンシに考慮することが必要である。特にlayer 7を含めた対応をとることで、サービス利用におけるレイテンシの影響の抑制を図ることが必要である。この点については、現在検討を進めているところである。

低消費電力サーバの利用: 低消費電力サーバ(たとえば、太陽光電池と充電可能電池の組み合わせで動くようなサーバ)群を利用することで、災害時や事故が発生したときの電力不足への対応を図る。サーバ群のサービス処理能力や消費電力をregistry で示しておくことで、利用可能なリソースの中で最適なシステムおよび情報基盤運用を可能にする。また、グリッドリソースとして低消費電力サーバを用いることで、処理あたりの消費電力(トランザクション/ワット)を高効率化することが可能である。

メッセージ・キュー: メッセージング・ネットワーク内に、メッセージ・キューを用意することで、要求処理に比して利用可能リソースが少ない場合に備えておく。これは、先に述べた各種データ処理を粒度の細かいサービスに分割し、それらを疎結合することと、**粒度**の細かいプライオリティー付けによって、実現可能となると考える。

提案手法の応用

今回の震災、原発事故では、様々な場所に避難した被災者の情報へのアクセスが十分にできないという問題が発生した。災害などによってシステムや通信基盤に大規模な障害が発生したときには、通常とは異なった場所からのアクセスが必要となる。この要求事項を実現するためには、様々な認証、認可、課金に対応できる情報基盤と情報システムの構築が必要である。認証に

ついては、本人確認と、属性確認によって、状況に応じたアクセス制御が必要となる。認可には、認証情報と認可ルールベースとの連携が必要不可欠である。このとき、サービスのサステナビリティ実現と柔軟性実現のためには、認証、認可、課金が密結合しているのではなくそれぞれが独立していること、そしてそれらを疎結合で自由に組み合わせられることが望ましい。認証・認可・課金情報を利用する様々なサービスは、認証、認可、課金サービスを適切に選択した上でそれらと疎結合するようにしておけば、システムの柔軟性や事業継続性を高めることができる。

これらのサービスの疎結合を、エッジで提供するのは、非常時の動作保証やメンテナンスの点からも好ましくない。そのため、これらサービスの疎結合はプロアクティブに情報基盤によって提供されるべきである。提案手法を用いることで、種々多様な認証・認可サービスの連携を実現することができる。ユーザの本人確認と属性確認を分離可能にしたうえで、利用するサービスごとに適切な認証・認可サービスを利用可能にすることが提案手法のcontent-aware network で実現することができる。SAMLなどを用いて認証情報をContent-awareネットワークに送り、異なった認証・認可サービスのインタフェースの相違を吸収する。認証・認可サービス間の連携と認証・認可サービスと各種サービスの連携も同一の基盤で実現することができる。

マイナンバーなどとの連携も提案手法では疎結合で実現する。現時点におけるマイナンバーのシステム検討案の一つでは、サービスの疎結合連携が大きな柱の一つとなっている[23]。

震災と原発事故に関連して進められている健康調査データストアは、そのデータ単独で利用されるよりは、関連する疾病に関する疫学データや医学研究情報、放射線被曝量、過去の気象データ、避難所での記録、アスベスト等有害物質の吸引可能性、などと連携した利用が中心となると考えられるが、これらは提案手法の疎結合連携や広域（疎結合）連携が有効となる。疫学調査では、ライフコースデータやそれに準じたデータなど個人情報が欠かせない。その一方、疫学調査の結果は、個々の個人を特定するような情報は不要である。様々な疫学調査を可能にしながら、個人情報の漏洩を防ぐ仕組みが必要である。また、疫学調査で得られた情報を治療などに使う場合には、その高い可用性が必要となる。これについては、前述したセキュアデータグリッドと関連サービスの疎結合、メッセージング・ネットワークによるマッシュアップ、フォーマット変換、アクセス制御の機能を、非IPネットを含む多様なネットワーク上のオーバレイネットワークで実現することを提案する。

結論

本研究では、メッセージング・ネットワークと仮想サーバ群、仮想ネットワークと、サービスの疎結合連携を用いることで、100年保つデータストアを実現する方法についての考察と提案を行った。サービスの疎結合連携による広域連携を可能にすることとあわせて、災害や事故が発生しても持続可能な情報基盤の実現方法について提案した。今後は、本提案に基づいた実証実験とその評価を行い、実運用に耐えるICT基盤を構築して行く予定である。

参考文献

[1] Darleen Fisher“US National Science Foundation and the Future Internet Design,” ACM SIGCOMM Computer Communication Review, Vol.37,no.3, pp.85-87, 2007

[2] A.Gavras, A. Karila, S.Fdida, .May, and M.Potts, “ “Future Internet Research and Experimentation: The FIRE Initiative,” ACM SIGCOMM Review, Vol.37,no.3, pp.89-92, 2007

[3] Council on Competitiveness ed., Innovate America, Council on Competitiveness US, 2005.

[4] Thomas Erl, SOA Design Patterns, Prentice Hall, 2008

[5] Martin Fowler. Patterns of enterprise application architecture, Addison-Wesley, 2002

[6] 福原英之,藤田龍太郎,杉本康則,林隆史, “メッセージング・ネットワークを用いたSOA構築,” 第2回国際CIO学会全国大会, 2007

[7] 福原英之, 藤田 龍太郎, 小瀬田 勇, 杉本 康則, 川内 見作,林 隆史, ”メッセージング・ネットワークを用いた地方公共団体システムの疎結合統合化,” 2007年度国際CIO学会秋季研究発表会

[8] 福原英之, 斎藤本和, 村上誠, 川内見作, 森田敬一, 小瀬田勇, 藤田龍太郎, 酒井琢夫,宮崎敏明, 斎藤梅朗, 岩瀬次郎, 林隆史, メッセージング・ネットワークを用いた情報ガバナンス, 2009年度国際CIO学会春季研究発表会

[9] G.Hohpe, B..Woolf, Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions, Addison-Wesley, 2003

[10] T. Hayashi., H. Fukuhara, R. Fajita, T. Miyazaki., and S. Saito, ″A Messaging Network to Realize an SOA-Based System,″. In Proc. of CIT2007,. IEEE, pp. 1083-1088.

[11] T. Hayashi. Zachman framework for realizing information security of local governments, JASI, 10(1):75-83, 2007

[12] T.Hayashi, “Schemes for Realizing Total Security in Information Systems, “ Proc. of 5th Intl. Conf. ICT and Higher Edu., June 2006

[13] 林隆史,福原英之,藤田龍太郎,川内見作,小瀬田勇,杉本康則, “メッセージング・ネットワークを基盤とした疎結合システムによる情報爆発対策および情報信憑性向上,” 国際CIO 学会ジャーナル, vol.2, 2008,

[14] 林隆史,後藤玲子,田中秀幸,須藤修,”電子自治体におけるSOA導入の課題と可能性,” 2008年日本社会情報学会合同研究発表大会

[15] J.Terazono, H.Fukuhara, I.Koseda, R.Fujita, T.Miyazaki, S.Saito, T.Hayashi, ″Service oriented architecture realized by a messaging network,″ NOMS 2010, IEEE , vol., no., pp.934-937, 19-23 2010

[16] T.Hayashi,H.fukuhara,K.Suzuki,T.Yamada,Y.Watanabe,J.Terazono, T.Suzuki,T.Miyazaki,S.Saito,I.Koseda,R.Fujita,J.Iwase,″A Network-Centric Approach to Sensor-data and Service Integration,″ SICE2011

[18] 村上誠, 福原英之, 川内見作, 宮崎敏明, 齊藤梅朗, 加羅淳, 岩瀬次郎、林隆史, “メッセージング・ネットワークを用いた知識社会情報基盤構築,” 2008 年JASI/JSIS 合同研究発表大会,pp.386-391, 2008

[19] P. Patrick. Impact of SOA on enterprise information architectures, Proceedings of the 2005 ACM SIGMOD international conference on Management of data, pp.844-848, 2005

[20] A. Nakao, R. Ozaki, and Y. Nishida, “CoreLab: an emerging network testbed employing hosted virtual machine monitor,” Proc. of ACM CoNEXT Conf., 2008, pp. 1-6.

[21] 須藤修,小尾敏夫,工藤裕子,後藤玲子 編著『CIO学―IT経営戦略の未来』東京大学出版会、2007

[22] 政府電子政府評価委員会（座長：須藤修）編『平成19年度電子政府評価委員会報告書』政府IT戦略本部IT新改革戦略評価専門調査会, 2008

[23] 政府次世代電子行政サービス基盤等検討プロジェクトチーム（座長：須藤修）編『次世代電子行政サービスの実現に向けたグランドデザイン』政府IT戦略本部、2008