RCSSディスカッションペーパーシリーズ
第45号　2006年9月

ISSN 1347-636X

Discussion Paper Series
No.45　September, 2006

電子自治体の構築とグリッドコンピューティング

小　林　孝　史

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1228
fax. 06-6330-3304

電子自治体の構築とグリッドコンピューティング

小　林　孝　史

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1228
fax. 06-6330-3304

電子自治体の構築とグリッドコンピューティング

小林孝史
関西大学ソシオネットワーク戦略研究センター研究員
関西大学総合情報学部助教授
E-mail: kobayasi@res.kutc.kansai-u.ac.jp

概要

電子自治体の構築のため，各業務システムにおいてレガシーシステムからの移行が進んでいる．しかし，単純にオープンシステムを導入しただけでは個別業務の最適化を行ったにすぎず，業務全体の最適化とはほど遠い．情報セキュリティ対策についても一定のレベルを達成する必要があり，個々のシステムで対策を行っていくには，担当者の負担が非常に大きくなる．

上記の問題を解決しながら電子自治体を構築していく際に，グリッドコンピューティングをどのように活用していくか，本論文ではその活用の可能性を示し，今後の電子自治体の構築の指針を示すことを目的としている．

KEYWORDS: 電子自治体，グリッドコンピューティング，サービス指向アーキテクチャ，エンタープライズ・アーキテクチャ

On the Building Methods of e-Local Government and Grid Computing

Takashi Kobayashi
Researcher, Research Center of Socio Network Strategies, Kansai University
Associate Professor, Faculty of Informatics, Kansai University
E-mail: kobayasi@res.kutc.kansai-u.ac.jp

Abstract

The migration processes of legacy systems and/or applications are going for the building e-local government. However, taking advantage of open systems is only making the optimization of each service, and it is far way from the optimization for whole of services. It is needed to achieve the apropriate level of information security countermeasure, and the person who take charge of information systems will be responsible for the countermeasure of every systems.

The aim of this paper is to show the availability of the grid computing and the guideline on the future system of e-local government in case of building e-local government while solving above problems.

KEYWORDS: e-Loval Government, Grid Computing, Service Oriented Architecture, Enterprise Architecture

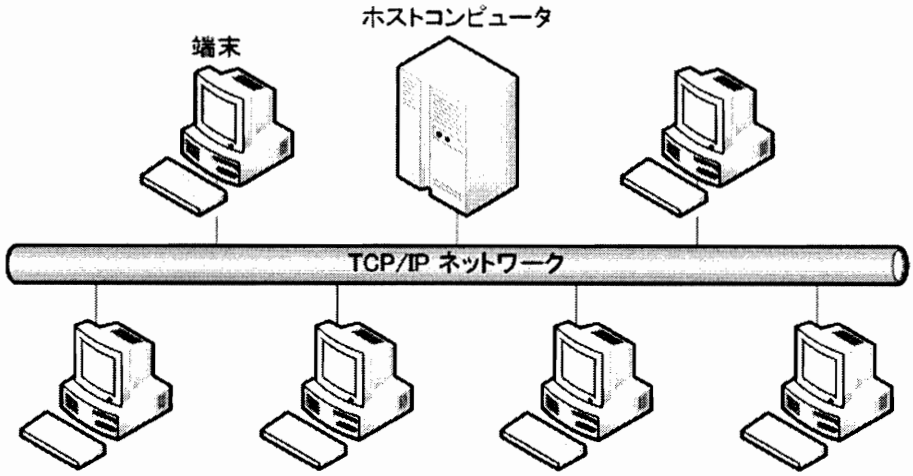

図 1: ホストコンピュータのネットワーク

1 はじめに

政府，自治体業務の電子化を進めるために，これまでさまざまな努力がなされてきた．その動きの中で近年では情報セキュリティを確保しつつ，旧来のシステムから新しいシステムへの移行を模索する段階にきている．また，各自治体においては [9] に示されるように，経営改革，情報キオスク，高度医療福祉，まちづくり，地域イントラネット，自動交付機，新世代地域ケーブルテレビ，光ファイバ網の整備など，電子自治体に資するさまざまな取り組みがなされている．電子政府，電子自治体の構築のためには，国民，市民の利便性を考慮に入れつつ，情報セキュリティに配慮して政府内，自治体内部の業務を最適化し，最高の効率を求める必要がある．

コストの問題から始まったといわれるレガシーシステムの置き換えは，業務の再構築または最適化へと動きが変化し，それに伴って，導入するシステムに対する考え方にも変化が求められている．業務の一部の電子化では不十分であり，縦割りをそのまま反映したシステムを構築しても全体最適化とはほど遠いシステム構成となってしまうため，業務を担っている現場が主体となってシステム更新を進めるボトムアップ的な手法だけではなく，トップダウン的にほぼすべての業務を網羅したシステム更新を進めることも必要である．

本論文では，これまでの電子自治体の構築方法と現状を俯瞰し，今後の電子自治体の構築に際して，考慮すべきこと，注意すべきことについての指針を示すことを目的とする．

2 電子自治体の構築

自治体のこれまでの業務を電子化し，業務効率の向上，つまり市民の利便性の向上を図ってきた．現在までに電子化が進み，さまざまな業務においてコンピュータを利用するようになってきている．これまでのシステム（レガシーシステム）では，ホストコンピュータを利用した中央集権型のオンラインシステムとして稼動している．これらのシステムにおいて，データは必ずホストコンピュータの中に留まり，人によって故意に漏洩させる以外に外界に出るということはありえなかった．現在でこそ，図 1 のようにネットワークプロトコルとして TCP/IP を使って，業務用のパーソナルコンピュータからホストコンピュータへ専用端末ソフトウェア（エミュレータ）を用いて接続しているが，基本的には閉じたネットワーク内で，端末はホストコンピュータの端末でしかない．

ホストコンピュータを中心としたいわゆるレガシーシステムで問題となるのは，電子自治体の構成要素である，市民からのアクセスを受け持つシステムとの親和性が非常に低いことである．市民はインターネットという手段を通じてアクセス行うが，レガシーシステムというのはインターネットとの接続ポイントを持たないのが通常のシステムパターンである．接続ポイントを持たないシステム同士を如何に接続するか，ということが大きな問題と

してあがってくる．また，ホストコンピュータを用いたシステムの場合，従来は職員自身がシステムを構築・運用・管理を行っていたが，現在ではその運用・管理の手間と制度・法令・条例改正に伴うシステム変更への対応の難しさから，パッケージソフトウェアを用いて若干のカスタマイズを加えたシステムへの移行も進んでおり，次第にホストコンピュータから離れていく傾向もある [3].

この問題を解決する 1 つの手段として，ホストコンピュータによるオンラインシステムを，いわゆるクライアント・サーバシステムへ移行するシステムが増えている．ただ単に業務システムを移行してシステムを刷新しただけではうまくはいかない．それは，レガシーシステムはホストコンピュータで構築されたシステムだけではなく，長期にわたる業務ノウハウの蓄積と暗黙知による業務の最適化を行っているからである．こういった背景が存在するため，近年では，組織全体の業務プロセスを最適化し，業務効率を最大限に引き出すための情報システムの構築方法論（Enterprise Architecture: EA）や，組織に関係するユーザーにサービスを提供するという観点から，サービスを中心とした情報システムの構築方法（Service Oriented Architecture: SOA）という考え方に基づいたシステム構築手法が出てきている．

3　情報セキュリティ対策とシステム構築の基準

業務を継続できる手段を講じること（可用性），業務上必要な情報に対する不正な手段でのアクセスを許さず，必要な時にアクセスできる手段を用意し維持すること（機密性），取り扱う情報が正しいことを保証すること（完全性），の 3 点を確保することが情報システムのセキュリティで求められていることである．しかしながら，情報セキュリティを確保すること（情報セキュリティ対策）と利便性とは相反する要素であり，対策を強めれば利便性は悪くなり，利便性を良くしようとすれば対策が弱くなる．情報セキュリティポリシーに基づいてシステムごとに情報セキュリティ対策を実施していく場合，実際の手順となるプロシージャのレベルの統一を行う必要もある．そのシステムの数が相当数に上る場合にもすべてのシステムについてヒアリング等を行って，そのレベルの統一を図らなければならず，情報システム部門や情報セキュリティの監督部署の負担は相当なものとなる．

一方，情報システムの構築手法は時代と共に変わっていく．システム稼働の際には技術的に不可能であったことも，年数を経ることによって可能になっていることも少なくはない．情報セキュリティのレベル向上や，プロシージャの更新とともに情報システムも進化させる必要がある．そのためには，システムを利用する部署の担当者のスキルアップを図ることはもちろんのこと，システム構築の専門家や情報システム部門等に意見を聞いたり，専門業者のコンサルティングを受ける必要がある．

また，個別システムの構築によってレガシーシステムの問題の解消を狙っている場合，そのシステムの情報セキュリティ対策のレベルがその組織全体のセキュリティレベルになってしまうことを十分に理解することが必要である．そして，それらの個別システムを構築することが本当に必要かどうか，別の業務で似たようなシステムがあるかどうか，というシステム化することの基準も必要である．その基準を設けることによって，個別の最適化ではなく，全体最適化へと通じるレガシーシステムの移行計画を立てることも必要である．

4　現行の情報システム

情報システムを利用した業務を行う場合，保守や維持・管理コストの問題がついてまわることとなる．情報システムを導入して運用を開始すればそれで終わりではなく，システムを健全な状態で維持したり，システムの入出力が正しいことを確認したり，日常的に稼働状況を確認したりする必要がある．これらについては，専門家や熟練者による作業が必要など，一般利用者が実施できるようなものでないことが多い．

これらの問題から，ホストコンピュータによるオンラインシステムから個別のシステムへ移行することを選択する業務が増えてきている．保守については，担当できる職員や技術者の不足が主な問題であり，維持・管理コストについては人材不足や独自開発したシステムの更新の際に膨大な移行コストがかかってしまうことがある．

本節では，現行の情報システムの現状の外観を述べる．

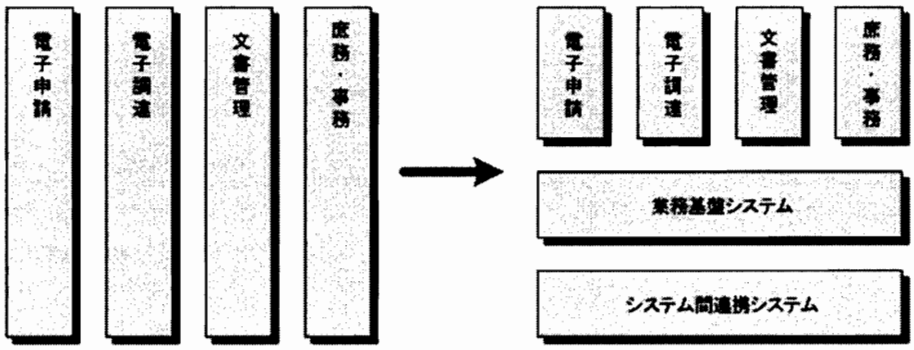

図 2: レガシーシステムとの差異

4.1 レガシーシステムとその移行

2005 年 9 月から 2006 年 8 月までの間に，JPCERT コーディネーションセンター（JPCERT/CC）から発表された JP Vendor Status Notes[1] の記事数は 200 を超える．JP Vendor Status Notes とは，日本国内のソフトウェア製品開発者の脆弱性対応状況を公開するサイトで，JPCERT/CC と情報処理推進機構が共同で運営している．1 年間でこれだけの脆弱性が開発者から報告され，それを利用する者やシステムは修正または対策を余儀なくされる．システムの数が増えれば増えるほど，それだけのコストが必要となるのである．対策を実施するための人的資源を投入できなければ，そのシステムを含む組織全体のセキュリティレベルはすぐには低下しないが長期的には低下し，組織の不利益をもたらす結果となる．

自治体に限らず，ある組織の情報セキュリティレベルはその組織内の個々の情報システムのセキュリティレベルに左右される．すなわち，1 つでも低いレベルのシステムがあれば，その組織のセキュリティレベルはそのレベルとして評価される．情報システムを個別に構築すると，その情報セキュリティレベルを維持するために個々に対策を行う必要があり，それが組織全体のセキュリティレベルを左右する．情報システムを構築する際にはこの辺りをよく理解した上で構築することが肝要である．関連する事項としては，情報セキュリティマネジメントシステム（ISMS）の認証を受けているからといってその組織全体の情報セキュリティ対策が万全かどうかは分からない，ということがある．ISMS 認証基準では，対象を限定することが可能であり，例え一部のごく内部的な情報を扱うシステムのみの認証でも構わないのである．ここに認証制度のトリックがある．

情報セキュリティレベルを一括して管理するためには，業務横断的なネットワークを構築し，それを基盤としたシステム構成を採用することが最もよいと思われる．業務横断的なネットワークとなるため，個々の業務間の連携の有無は確実に規定する必要があるし，規定以外でのアクセス許可や拒否はあってはならない．この構成とすることにより，個々のネットワークを持つことなく，それぞれの業務サポートのための情報システムを持つことができ，将来的に連携して作動することが必要になった場合でもスムーズな移行が可能となる．

情報システムを連携する際に考えなければならないことは，それぞれの情報システムの接続ポイントがアーキテクチャ独立になっているかどうか，ということである．それは，情報システムの寿命が尽きる前にリプレースを行う必要があるが，そのリプレースによって連携作用が一時的に失われることはあってはならない．そのためにも，接続ポイントはどのアーキテクチャでシステムが構築されたとしても，そのアーキテクチャに依存することのないようにする必要がある．連携作用が一時的に失われる，ということは，そのシステム間の連携ができなくなるということであり，これはそのシステムの可用性を確保できていないということになる．この傾向は，これまでのように，システムのアーキテクチャを変更する際に頻繁に起きることであったわけであるが，近年のサービス指向アーキテクチャなどでは，サービス基盤とサービス提供に分けて構築することが可能になっているため，そういった心配はなくなってきている．しかし，極小規模のシステムの場合，予算上の理由により SOA 的な構成がとれないこともあって，新しい流れに乗っていくことが難しい場合が多い．

図 2 では，従来のシステムから最適化後のシステムの移行に示す．従来のシステムでは，各システムが部分的

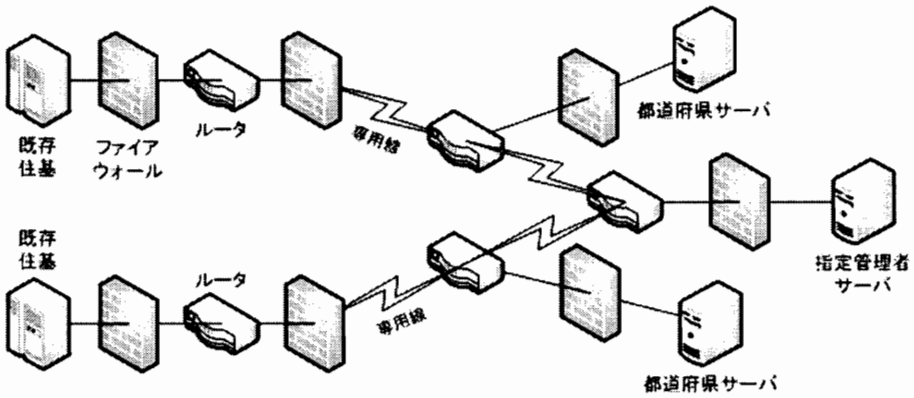

図 3: 住民基本台帳ネットワークの構成

に最適化した状態で構築されており，正に，業務の縦割りをシステムにそのまま当てはめた状態になっている．それと比較して最適化後のシステムでは，関係する業務のすべてが最適化され，業務横断的な業務基盤システムが備わっている．この業務基盤システムには，申請業務に必要な電子決済や手数料収受のシステムも含まれており，既存業務をもこのシステム上で行うことのできる設計となっている．このようなシステム構成へ移行することで，基盤システムの開発コストを 1/3 から 1/5 に下げることができるといわれている．その理由としては，従来から行われているシステムを移行する際，そのシステムに習熟しているなどの理由から随意契約を行って現在のシステムから大きく変更しない場合がかなり多いことが挙げられる．特にレガシーシステムではその割合は多く，しかも日本の場合，レガシーシステムへの IT 投資は合衆国の 3 倍，欧州連合の 2 倍程度になっているといわれており，このコストを下げることができれば，IT 投資もかなり低くなると考えられる．

業務基盤システムはその存在だけで十分ではない．さらにその下部に位置するシステム連携システムが重要な要素となる．システム間連携システムは共通のデータベース等のシステムをつなぎ合わせる仕組みを持ち，システムが変更になったとしてもそのインターフェイス部分が変わらないような設計となっている．従って，下部システムが変更になったとしても，業務基盤システムのインターフェイスは変わらないため，個々の業務システムは業務基盤へのアクセスを考えた設計を進めればよいことになる．

4.2 住民基本台帳ネットワーク

住民基本台帳ネットワークは，平成 11 年の住民基本台帳法の改正によって，住民票の記載事項として新たに住民票コードを加え，住民票コードを基に，行政機関に対する本人確認情報の提供や市町村の区域を越えて住民基本台帳に関する事務の処理を行うため，地方公共団体のシステムとして各市町村の住民基本台帳のネットワーク化を図ったものである．簡単な構成図を図 3 に示す．

各方面で賛否両論が議論され，裁判で争われているところでもある [8] が，基盤技術としては必要不可欠なものである．ただし，「住民票コード」が追加されたために問題視されている．そもそもデータベースを構築する際，格納するデータには何らかの識別子（数字，文字その他）が割り振られる．その識別子は格納するデータの重複チェック等に用いられているものであるが，通常は公開せず内部コードとして利用するのみである．住基ネットにおいてはその内部コードであるべき「住民票コード」を公開した点に政策的誤りがあると考える．

住民基本台帳ネットワークを基盤システムと位置づけることができるが，地方公共団体全体で共同利用している「共同利用データセンター」と見ることもできる．ただし，全国規模のシステムであるため，端末の設置されている各地方自治体のセキュリティレベルが全体のセキュリティレベルに反映する．従って，個々の端末周辺のセキュリティレベルを合わせるために，情報セキュリティ監査が行われている．この監査結果によって個々のセキュリティレベルを確認し，全体のセキュリティレベルを維持することにつなげている．

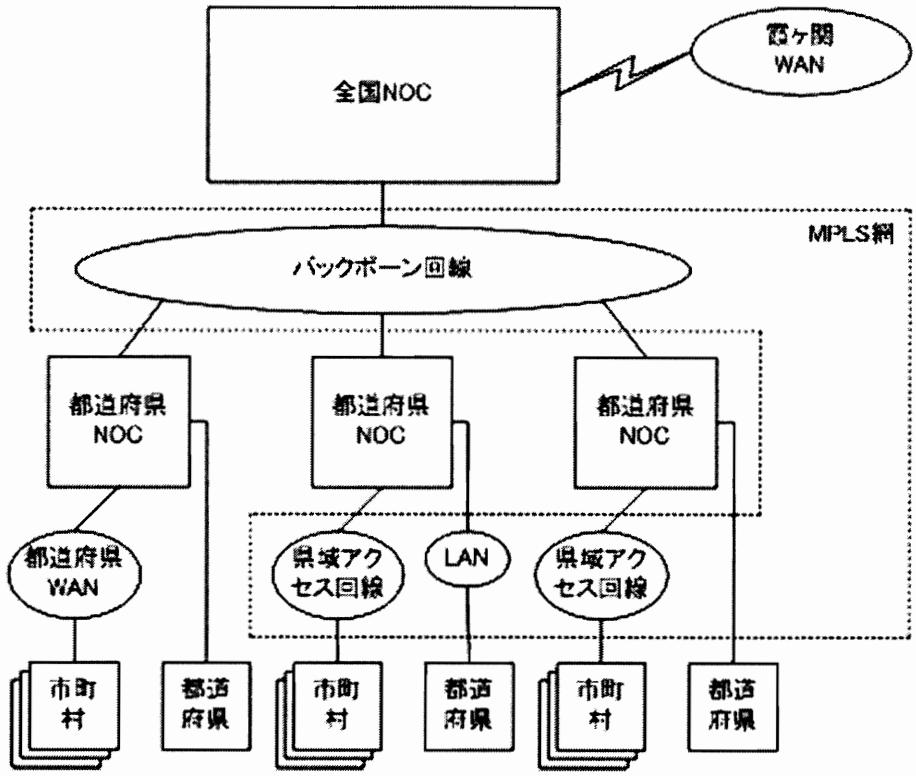

図 4: 総合行政ネットワークの構成

この住民基本台帳ネットワークは，地方自治情報センター（LASDEC）が運営委託を受けて運用を行っているが，地方公共団体に設置された機器については各地方公共団体で運用を行っている．地方公共団体側の設備としては，コミュニケーションサーバ（Communication Server: CS）とファイアウォール（FireWall: FW）があり，この設備を介して地方公共団体側で運営している既存の住民情報システムとの情報交換を行っている．都道府県サーバと指定情報処理機関の運営する業務/DB サーバには，いわゆる 4 情報（氏名・住所・性別・生年月日），住民票コード及びこれらの変更情報のみを保有している．

電子政府・電子自治体を実現するためには，住民情報の確認を何らかの形で実施することが不可欠であるが，そのためには電子的な受付システムが住民情報を確認できる状況を作り出すことが必要である．個人情報保護の観点から，都道府県や各地方公共団体側のサーバを直接受付システムと結合することはできない．従って，別の手段を用いる必要があるが，その際の候補となるのが，4.4 節で述べる汎用受付システムである．この汎用受付システムを単なる受付システムとするだけでは不十分で，住基ネットシステムの指定情報処理機関として認定される必要がある．

地方公共団体や住民情報を必要としている業務を行う機関が単独で指定情報処理機関として認定されるように設備の整備を進めるには莫大な費用と時間がかかることは明白であり，ここでも共同利用の形態を採用する以外にはないのではないかと考える．

4.3 総合行政ネットワーク（LGWAN）

LGWAN については，中央省庁と地方自治体とを結ぶ閉じたネットワークとなっている．文書交換や掲示板等の利用を行うことを想定して構築しており，現在は公的個人認証の鍵証明等に主に用いられている [5].

LGWAN は図 4 に示すように，霞ヶ関の政府省庁と都道府県 NOC （Network Operation Center）をつなぎ，さらに都道府県 NOC に各地方自治体のシステムを接続している．バックボーン回線と各都道府県 NOC の間は

IP-VPN 接続により他のネットワークからの覗き見もできないようになっている．バックボーン及び県域アクセス回線は MPLS（Multi-Protocol Label Switching）技術を用いた，特定の NOC 以外との通信ができないような措置がとられており，安全な通信路が確保されている．

各地方公共団体側の行政用ネットワークから何らかの手段を用いて LGWAN と通信ができるようになっているが，LGWAN に接続している別の地方公共団体へのアクセスは不可能である．主に，(1) 基本サービス（文書交換，電子掲示板），(2)LGWAN-ASP，の利用のためのネットワークである．また，地方公共団体と霞ヶ関 WAN を結ぶアクセス回線としての役割もあり，平成 15 年度までにすべての地方公共団体が参加するに至っている．

一般的には，地方公共団体の行政ネットワークが LGWAN と接続されることになるので，LGWAN のセキュリティレベルは地方公共団体のセキュリティレベルに左右される．

4.4 共同運営データセンター

電子自治体構築に向けた取り組みのうち，申請・届出等の手続きをオンライン化する汎用受付システムの導入状況は，都道府県で 78.7%，市町村で 20.4%となっている[1]．この汎用受付システムの実現形態としては，独自方式，共同方式および併用方式が基本仕様として考えられている [11]．どの方式を採用してもよいが，パイロット事業でも採用したように，共同方式による実現が最も現実的であろう．

電子自治体の構築に共同利用システムを活用することで，初期投資は 2 年程度で回収でき，長期的に見ても相当に有利であるという分析結果が出ている [12]．つまり，いくつかの自治体が共同で運用するシステムを構築し，それを一斉に利用することにより，費用対効果は元より，各自治体の電子化に大きく寄与すると言える．また，参加する自治体が多ければ多いほどスケールメリットを発揮し，各自治体の金銭的な負担は軽くなる．

5 グリッドコンピューティング

グリッドは「電力網（グリッド）からの電力の取り出し」から発生した用語であるが，これを情報システムに導入すると，「高度にネットワーク化された情報システムからのデータ，サービスの取り出し」となる．情報システムでいうところのグリッドには，データベースグリッド，リソースグリッド，コンピューティンググリッド，など設計者により様々な解釈がある．中には冗長構成を採っただけのものもあり，グリッドとクラスタシステムの境界は曖昧になっているが，広い意味でのグリッドと捉えればよいであろう．

前節までで主張してきた，バックエンド側のシステムや，汎用受付システムを共同利用型のシステムとして構築するということに関連してであるが，これらのシステムは基本的に 24 時間 365 日稼働することに努めなければならない．そうして初めて，いつでもどこでもサービスを受け付けるシステムとして成立する．従って，情報セキュリティの 3 本柱のうちの 1 つである「可用性」を実現するために，ノンストップサービスが可能なシステムであることが前提となる．グリッド技術を利用してこれらのシステムを構築することにより，これらのシステムでは常にサービスを継続できることが期待できる．

また，共通基盤システムを導入する際にも，グリッド技術は共通基盤システムとの親和性が非常に高いと考えられる．グリッドシステムから取り出されるのはサービスやデータであり，ユーザーインターフェイスを変えることなく，バックエンドのシステムを取り替え可能となり，個別導入のシステムと比較して導入コストの面などで，グリッド技術を利用した基盤システムの構築は非常に有利であると言える．

図 5: Linux からの Windows 利用

6 構築事例

6.1 シン・クライアントを採用する場合

Windows Server のターミナルサーバ機能を利用し，複数の利用者が同時に同じ Windows Server 上で作業ができるようにする．利用者の用いる端末には情報は格納されず，すべてサーバ内に保存されるため，情報漏洩の可能性が非常に低くなる．

図 5 は，Linux PC を端末として Windows サーバを利用した画面である．RDP（Remote Desktop Protocol）を利用した遠隔接続によって，Windows 以外の環境からも Windows を遠隔操作することが可能になっている．このタイプのシン・クライアントの場合，通常の Windows PC とほぼ同じインターフェイスで利用ができ，かつ，情報は Windows サーバのみに記憶されるという利点がある．作業負荷はすべて Windows サーバが担当し，クライアントには描画処理のみを担当すればよいことになる．RDP に対応したソフトウェアとしては，UNIX/Linux 用の `rdesktop`[13]，WindowsXP Professional に付属するリモートデスクトップ接続 [14] がある．これらを実行するコンピュータは少々性能が低くても，実際の処理はサーバ側で行うため，端末の長寿命化や再利用をしやすくなり，トータルでの総コストを抑制できる効果もある．

グリッドベースのシステムを構築し，そのシステムへのアクセス手段としてシン・クライアントを利用する．そうすることにより，必要な情報に必要なときにセキュリティを確保した状態でアクセスが可能になる．バックエンドに配置されたグリッドによって，バックエンドのシステムの一部に障害が発生してもフロントエンドの端末側では業務を続けることができる．クライアント側には特に性能は求められず，サーバの性能をクライアントでも利用することが可能になるため，サーバ資源の有効活用と同時にシステム資源の最適化も図ることができる．

また，サーバベース・コンピューティングの別の利点としては，ソフトウェア資源の一元管理も同時に実現できることがある．コンピュータの台数が多くなれば多くなるほど，そのソフトウェア管理，ライセンス管理が難しくなるが，サーバに集中した形で管理できればライセンス数の管理のみでよくなり，かかる経費はクライアントの台数および利用者の人数には無関係になる．特にオープンソースでコピーフリーのアプリケーションソフト

[1]総務省情報通信白書平成 18 年度版

ウェアの場合では，頻繁に発生するアップデートをサーバ上にインストールされたものに適用するのみでよくなり，最新版への維持・管理コストもかなり減少する．スタンドアロン型のクライアントの場合，台数が増えれば増えるほど，その利用ソフトウェアの管理コストが増えていくが，シン・クライアント型の場合は，サーバの台数のみに依存し，クライアントの台数には無関係となる．

ただし，シン・クライアントをクライアント端末に採用すると，端末を持ち運べない，ネットワークにトラブルが発生すると使えない，という問題も考慮に入れる必要はある．その場合は，シン・クライアント端末以外にスタンドアロン型の端末も用意し，それを何らかの形で利用することができるようにすればよいと考える．通常はシン・クライアントを繋いでいるが，トラブルの際には同じ回線を使って，VLAN 技術により接続する先を変更するという運用も可能である．

6.2 Web 2.0

最近では，電子掲示板（BBS）に始まり，コンテンツ管理システム（Contents Management System: CMS），ソーシャルネットワークサイト（SNS），Weblog，日記サイトなど，個人でホームページを開設し，さらに他の人にも使ってもらう（記事を投稿してもらう）などの双方向性を持ったシステムが多数出現している．この流れ全体をさして Web 2.0 と呼ばれている．1.0 がサーバからの情報提供を中心としたものと考え，それを基準とした「Web 2.0」という考え方である．

さらに，通常はコンピュータ上でソフトウェア（アプリケーション）を起動して作業をするが，そのアプリケーションを Web アプリケーションとして実装し，その際にブラウザを JavaScript でコントロールし，さらにブラウザとサーバの間で通信を行った結果をブラウザに反映するという手法を採用したものが増えている．この仕組みを AJAX（Asynchronous JavaScript + XML）フレームワークと呼ばれている．ブラウザとサーバの通信に XML が使われ，サーバから送られてきた結果を JavaScript で処理してブラウザに反映するという仕組みである．

この AJAX フレームワークを用いることにより，サーバすら意識することなく，ユーザーとブラウザの間で作業が進んでいくことになる．フロントエンドとバックエンドをつなぐ仕組みとして，この AJAX フレームワークを用いることにより，ユーザーはバックエンドにあるシステムを意識することなく，アプリケーションを利用できる．この場合も，データ自体はサーバで保管することになり，明示的にダウンロードしない限りは情報漏洩の可能性は低くなる．

7 おわりに

共同利用システム，共通基盤システムおよびグリッドシステムに共通した事項であるが，そのシステム仕様のオープン化は絶対条件である．暗黙知による業務もほぼ完全にシステム化することによって，初めてこれらのアーキテクチャが可能になるため，個別業務の最適化という事項にとらわれることなく，全体最適化のための行動を起こすことが必要である．

また，これらのシステムは電子政府・電子自治体の基盤となるため，サービスの提供が確固たるものでなければならない．そのサービスの提供が設計通りに行われているか，日常的な確認だけでなく，システムとしての確認手法の確率も必要であると考える．

参考文献

[1] JPCERT/CC, "JP Vendor Status Notes", `http://jvn.jp/`.

[2] 総務省, "地方公共団体における情報セキュリティポリシーに関するガイドライン", 平成 15 年 3 月一部改定.

[3] 総務省, "電子自治体推進指針", 平成 15 年 8 月.

[4] 総務省, "個人情報保護強化技術実装システムの開発・実証プロジェクト報告書", 平成 18 年 3 月.

[5] 総務省, "総合行政ネットワークの在り方に関する調査研究報告書", 平成 17 年 3 月.

[6] 情報化推進国民会議編: "電子自治体入門", NTTP 出版, 2003.

[7] OA 情報化政策検討論集会実行委員会/自治体問題研究所編: "IT・電子自治体をどう見る", 自治体研究社, 2001.

[8] 畔上文昭: "電子自治体の○と×", 技報堂出版, 2006.

[9] 市町村自治研究会編: "電子自治体への取り組み", 日本加除出版, 2003.

[10] 藤谷護人他著: "地方自治 IT 法務大全", 日経 BP, 2004.

[11] 自治事務等オンライン化推進関係省庁連絡会議, "地方公共団体における申請・届出等手続に関する汎用受付システムの基本仕様（第二版）", 2003 年 3 月.

[12] 上山晃, "市町村共同利用による費用削減効果と移行時期～主に電子調達を対象に", 電子自治体のシステム構築のあり方に関する検討会第 9 回会合資料, 2006 年 5 月 31 日.

[13] "rdesktop: A Remote Desktop Protocol client", `http://www.rdesktop.org/`.

[14] "機能別紹介 - リモートデスクトップ", `http://www.microsoft.com/japan/windowsxp/pro/business/feature/remote/remotedesktop.mspx`.