CDA R2 に準拠した個人提供用健康診断結果報告書を利用した個人健康情報管理システム

喜多 紘一[1)] 平井 正明[2)] 鈴木 裕之[1)] 谷内田 益義[1)] 山口 雅浩[1)]
小尾 高史[1)] 大山 永昭[1)]
東京工業大学[1)] HL7 Japan CDA SIG WG1 Leader[2)]

The personal health data referring system conforming to a health checkup report standard for personal use based on CDA R2

Kita Kouichi[1)] Hirai Masaki[2)] Suzuki Hiroyuki[1)] Yachida Masuyoshi[1)]
Yamaguchi Masahiro[1)] Obi Takafumi[1)] Ohyama Nagaaki[1)]
Tokyo Institute of Technology[1)] HL7 Japan CDA SIG WG1 Leader[2)]

Medical examination result reports with image data such as chest films and a wave pattern or of the electrocardiogram could be provided electronically to an individual using an "electronic post-office box" mechanism. These reports will be proposed in the case of medical treatment at a hospital. The standard formats were proposed. A card with PKI for the certification as an access card to the system is effective and dynamic on-demand VPN is useful as a secure network for this purpose.

Keywords: CDA R2, Medical helth examination, Electronic POB, Health checkup report

1. はじめに

1.1 個人提供用健康診断結果報告書の電子的提供

日本HL7協会のCDA SIGでは患者診療情報提供書のCDA R2準拠フォーマットでの標準化を行い、Helics規格としても採用された[1]。一方、特定健診による生活指導が2008年より始まり、健診データの保険者による保管と健診機関からの電子データの送付が計画され、そのフォーマットの規格化が進められている[2]。特定健診でのフォーマットは波形や画像をデジタルで提供することを目的としていない。また、健康保険組合等が健康指導を行う為のもので、個人へ提供し、個人が健康管理や診療に活用することを直接の目的としていない。そこで、特定健診のフォーマットと互換性があり、必要により波形や画像もデジタルで提供可能で且つ、個人に提供することを目的としたフォーマットを提供することを目的とした。

1.2 重点計画-2007

一方、IT戦略本部でまとめられた[重点計画ー2007]では「個人が自ら健康情報を管理し健康管理等に活用するための仕組みの確立」および「国民視点の社会保障サービスの実現に向けての電子私書箱(仮称)の創設」が歌われている[3]。前者は「個人が健康情報を電子的に入手し、自ら健康管理や診療時における提示等に活用できるよう、健康情報入手及び管理に関するルール等の仕組みについて、2008 年度までに方針を示す。」となっている。具体的な動きとして「静岡県版電子カルテシステム」[.4]や「厚生労働省の電子的診療情報交換辞表(SS-MIX)では診療情報をCD-Rに書き出して提供することを始めている。また、経済産業省では相互運用性実証事業の中の「電子診療情報システムの実証事業」で診療情報提供書を電子的に患者に渡す実証事業を行った。電子私書箱は「医療機関や保険者等に個別管理されている情報を、希望する国民が自ら入手・管理できる「電子私書箱(仮称)」を検討し、2010 年頃のサービス開始を目指す。」となっていて検討が始まった段階である。

1.3 ヘルス情報共有データベース基盤としての4つの観点

ヘルスケア分野で情報を共有することがはじまっているが、図1に示すように4つの観点に整理される。即ち「地域連携クリティカルパスのための野情報共有」、「かかりつけ医のための情報共有」、「行政、研究、経営管理のための情報共有」および「個人の自己健康管理のための情報共有」である。前者の3つは今まで議論がなされ実際に実現しつつあるが、最後の観点のものは検討が始まった段階である。

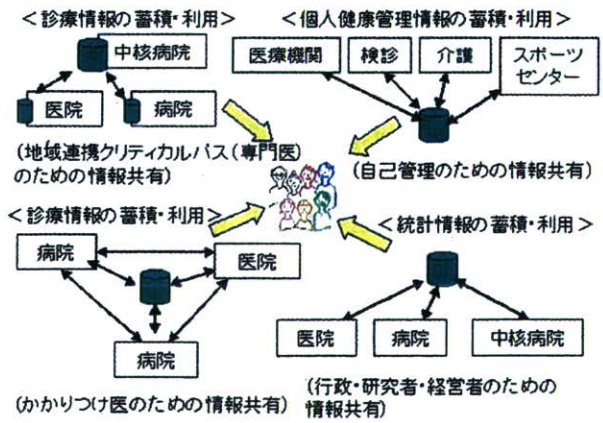

図1 ヘルス情報共有のための4つの基盤の観点

健康情報の個人の自己健康管理を電子的に配送し、受診者がダウンロードしたり、サーバに登録し、診療や健康維持のために必要なものだけを整理して医療機

関や自宅で参照することが可能である。こうした「個人健康情報管理システム」の電子私書箱による構想も合わせて提案する。

2. 方法

個人提供用健康診断結果報告書フォーマットは特定健診フォーマットの規格との整合をもたせた。波形や画像も提供できるようにCDAの外部参照ファイルとした。受診者情報、報告書作成機関情報、検査結果コンポーネント、問診結果コンポーネント及び判定結果コンポーネントは特定健診のフォーマットと同様とした。

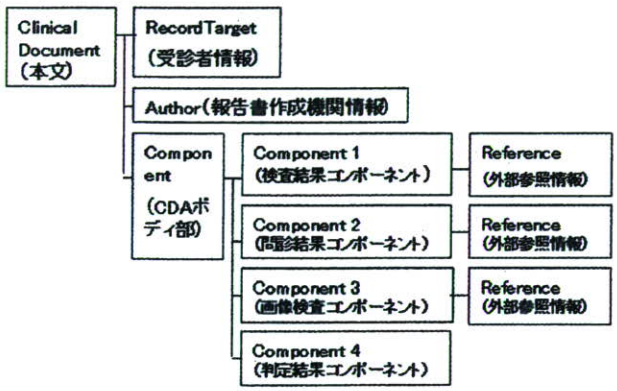

図2 個人提供用健康診断結果報告書フォーマット

本規格はHL7 CDA R2に基づいて規定し、且つHelicsで採用されたている患者診療情報提供書の署名、タイムスタンプ、暗号化方式に準じた。電子私書箱は重点計画等の発表資料を参考に調査した。

3. 結果

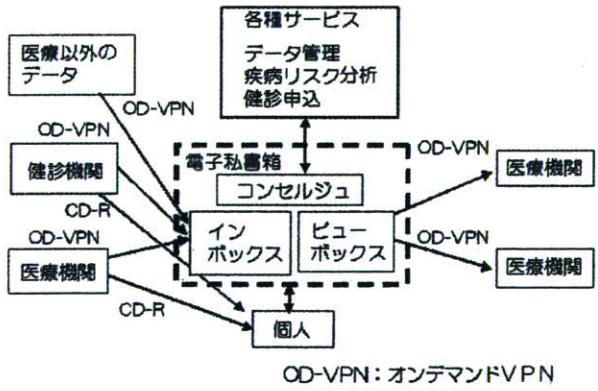

図3 電子私書箱構想による実現

個人提供用健康診断結果報告書はCD-Rへ書き込み付属のViewerで表示を行った。検体検査の表示は数値データだけでなく経年変化がグラフで確認でき、心電図やDICOM画像は専用のビューワーでそれぞれ確認することができた。「個人健康情報管理システム」は図3に示すように健康診断結果を受取るところ（インボックス）、及び病院で個人が参照し（ビューボックス）、結果から疾患リスクの評価や健診申込等のサービスを行う部分（コンセルジュ）に電子私書箱構想を利用した。健診機関等から健康・医療情報を電子私書箱へ提供するネットワークはHPKIを利用してVPN機器の所属する機関の属性を確認可能とするためダイナミック・オンデマンドVPNに機能追加[5]を行うこととした。電子私書箱のデータを医療機関側で参照する場合もアクセスするネットワークは同様のネットワークを使用することとした。

4. 考察

CDAフォーは日本HL7 CDA-SIGに提案を行いスキーマとの整合性のチェックを行っている。特定健診とのハーモナイゼーションを行うために全体を「HL7CDA健診情報規格群」として一体化した以下のような規格体系で検討している。Part1が本研究のフォーマット、Part2が特定健診のフォーマットにあたる。

1) Part1－通則－
2) Part2－個人提供用健康診断結果報告書－
3) Part3－健診情報ファイル仕様規格－

HPKI署名や署名検証画面がわかりにくいので印鑑の押印や検証の感覚で使えるためには今後の検討が必要である。個人健康情報管理システムは電子私書箱で暗号化されたデータを復号する場合の安全性確保の検討が必要である。

5. まとめ

重点計画-2007で示されている「健康情報の入手及び管理システム」の一つとして「電子私書箱」構想を利用して健康診断結果報告書を電子的に提供し、さらに希望者には心電図の波形や胸部写真等の画像データも入手し、診療の際に病院で提示できることを示した。また、システムへのアクセスカードとして認証用のPKI入りカードが有効であり、セキュアなネットワークとしてダイナミック・オンデマンドVPNを利用できることを示した。今回は個人提供用健康診断結果報告書を電子化するためのフォーマットを利用してその実現性の評価をおこなった。今後はさらにフォーマットのスキーマとの整合性の精査を行っていくとともに、健診以外のデータも提供可能となるよう検討を行う。

6. 謝辞

「個人提供用健康診断結果報告書フォーマット」の提案およびCD-Rへの書込等の基礎技術開発は情報通信研究機構委託研究：「ネットワーク認証型コンテンツアクセス制御技術の研究開発」において行われた。また、電子私書箱の調査は文部科学省科学技術振興調整費支援を受けている。

参考文献

[1] 制定済標準規格.http://www.hl7.jp/intro/index.html.
[2] 健診データの電子的管理の整備に関するホームページ.http://tokuteikenshin.jp/.
[3] 重点計画－2007.http://www.kantei.go.jp/jp/singi/it2/kettei/070726honbun.pdf.
[4] 静岡県版電子カルテシステム.http://www.mi.hama-med.ac.jp/emr/.
[5] 喜多紘一他5名.HPKIとダイナミック・オンデマンドVPNとの連携によるセキュアな医療ドメインネットワーク.第27回医療情報学連合大会.

HPKIとダイナミック・オンデマンドVPNとの連携による セキュアな医療ドメインネットワーク

喜多 紘一[1] 鈴木 裕之[1] 竹田 忠雄[2] 猪俣 彰浩[3] 島田 宏[4] 有馬 一閣[5]
東京工業大学[1] (株)NTTPCコミュニケーションズ[2] 富士通(株)[3]
Heasnt 技術委員会 主査[4] (株)NTTデータ[5]

A secure health domain network by cooperation with HPKI and dynamic on-demand VPN

Kita Kouichi[1] Suzuki Hiroyuki[1] Takeda Tadao[2] Inomata Akihiro[3]
Shimada Hiroshi[4] Arima Kuniharu[5]
Tokyo Institute of Technology[1] NTTPC Comunications[2] Fujitsu Limited[3]
Heasnet Technical Committee chairman[4] NTT DATA CORPORATION[5]

The VPN service provider judges it whether it is connection application from the VPN equipment which is administrated by a medical institution with HPKI certificate and admits connection to medical database. By this method, secure network environment of the free access for the medical institution by the patient that is a infrastructure between medical associated institutions are realized.

Keywords: HPKI, Dynamic on-demand VPN, XACML, SAML, Secure network

1. はじめに

1.1 ダイナミック・オンデマンドVPNのねらい

医療情報システムの安全管理に関するガイドライン第2版」では、「外部と個人情報を含む医療情報を交換する場合の安全管理に対する最低限のガイドライン」として以下の8項目をあげている。

1) セキュアなネットワーク経路を確保
2) データ送受信の拠点の出入口、使用機器で利用者の必要な単位で相手確認
3) 正規利用者、許可機器への成りすまし防止
4) ルータ機器は安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPN間で送受信が不可となる経路設定
5) 送信元と相手先当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施
6) 医療機関等、通信事業者、システムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社などの組織間で責任分界点、責任の所在を契約書等で明確化
7) リモートメンテナンスを実施する場合は不必要なログインの防止
8) 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認

また、「外部との医療情報の交換」に関して、以下の5通りの接続形態が記述されている。

1) クローズドなネットワークで接続する場合
   a) 専用線で接続されている場合
   b) 公衆網で接続されている場合
   c) 閉域IP通信網で接続されている場合
2) オープンなネットワークで接続されている場合
   a) 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保した形態でサービス提供する場合
   b) 医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合

ダイナミック・オンデマンドVPNはこの中の2aにあたる形態のネットワークであり、通信経路上の脅威の対策のための管理責任の大部分をこれらのVPNサービス提供者に委託できる。最低限のガイドラインの1番目に対しIKEとIPSecによるVPN方式により対応している。これにより、以下にあげる医療分野におけるネットワーク要件を満たし、ガイドラインに適合したネットワークの提供を目指している。

1) 安全な通信
2) 大容量データの高速通信
3) メッシュ型ネットワークの実現と拡張性
4) 参加メンバ(利用者、組織、機器)の真正性保証
5) セキュアネットワーク接続に関するコスト削減

1.2 ダイナミック・オンデマンドVPNの手続き

1.2.1 VPNサービス利用申請

VPNサービス利用申請は電話で言えば電話番号を入手することに当たる。サービス利用者は、機器証明書が搭載されたVPN機器を購入(入手)し、ダイナミック・オンデマンドVPNサービス提供者(以降サービス提供者)に、VPNサービス利用申請をする。サービス提供者は一階層目のPKIで機器証明書により機器の正当性を認証し、VPNサービスの為のサービス証明書をネットワーク経由でVPN機器にダウンロードする。

1.2.2 接続許可申請

接続許可申請は電話で言えば相手の電話番号の入手や、相手に自分の電話番号を連絡することにあたる。ダイナミック・オンデマンドVPNの場合、双方から接続をしたい機器を申請、両方から申請(許可)されて

いるものに対してサービス提供者はVPN接続に必要な「接続情報」をVPN機器にダウンロードする。

1.2.3 通信の開始

サービス利用者は通信開始時、通信相手を選択しIKEを行い相手とIPトンネルを形成し、通信を開始する。ダイナミック・オンデマンドVPNは2階層PKIによりルータの接続パラメータをオンラインでダウンロードする。接続相手を変える場合もパラメータをダウンロードすれば良いのでN:NのVPN接続が可能となる。

1.2.4 HPKI連携の目指すもの

現状のダイナミック・オンデマンドVPNは安全性の観点から、接続元および接続先の双方から接続許可が出されるまで、接続を許可しない。従って患者データが保存された医療関連データベース(以降MDB)に患者が診療を受けにきた医療機関からアクセスする場合を想定すると、あらかじめ事前にMDBから接続許可のあった医療機関しかMDBと通信できないことになる。いいかえれば、患者はあらかじめMDBとの接続を許可された医療機関へ行かざるをえずフリーアクセスの原則がみたせなくなる。本研究ではHPKIを利用して課題を解決できる方式を提案する。

2. 方法

2.1 HPKI署名付サービス利用申請書

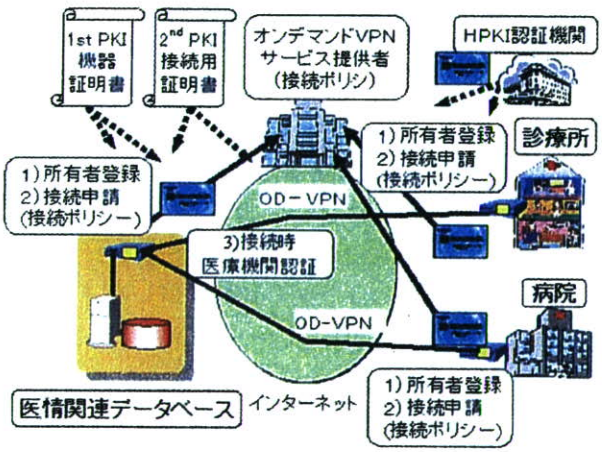

図1 HPKIを利用したダイナミック・オンデマンドVPNの概要

医療機関がVPNサービス利用申請としてVPN機器の登録情報をVPNサービス提供者に送付する際、申請書に医療機関の責任者用のHPKIで署名する。MDBは接続申請時に接続申請する機器がHPKI付申請のものであれば接続を許可することをVPNサービス提供者に申請する。VPNサービス提供者はあらかじめHPKI署名付申請で医療機関であることを登録したVPN機器からの接続申請かを判定し、MDBへの接続を許可する。この場合、接続の合意はMDBのポリシーと一致することにより事前確認が双方で取られているものとみなす。このポリシー制御の考え方はXACMLの概念に類似している。

2.2 XACMLおよびSAMLの概念の利用

XACMLはPDP(Policy Decision Point)、PEP(Policy Enforcement Point)およびPAP(Policy Administration Point)のキープレーヤを定義している。[1]

ダイナミック・オンデマンドVPNではPEPは接続許可申請に対し接続情報のVPN機器への配布点にあたる。PDPはポリシーに基づく接続許可の判断す点にあたる。PDPはPAPのポリシーに基づき判断を行う。

XACMLは3つのContextを定めている。PAPからPDPに示すルールやポリシーを記述するための「XMLスキーマ」、PEPがアクセス要求者の属性情報を記述してPDPに提示する「要求Context」およびPDPがPEPに返す認可決定の「応答Contextのスキーマ」である。

「ポリシーを記述するスキーマ」はMDBの接続許可申請時に「MDBに対して接続許可申請するVPN機器がHPKI付申請のものであれば接続を許可する」ポリシーをVPNサービス提供者に申請するときの構文の考え方に使用できる。

また、SAMLでは「認証オーソリティ」と「属性オーソリティ」がAssersionをResponseとして応答するときにオーソリティの署名つきで応答する。これは「VPNサービス利用申請時、申請書に医療機関の責任者用のHPKIで署名する」時の構文の考え方に利用できる。ただし、PDPが署名の属性も利用するところが異なっている。

3. 結果

本方式により、医療機関からのアクセスであれば、事前のサーバ側からの個別接続許可がなくても、接続を可能とすることができ、患者の医療機関に対するフリーアクセスの環境を実現でき、医療関連施設間のネットワーク基盤すなわち医療ドメインネットワークを形成することができる。

4. 考察

医療機関というだけでMDB側が接続を許可するのはダイナミック・オンデマンドVPNのセキュリティポリシーの制御としてものたりないとの考え方もある。その為にはhcRoleを使って、例えば薬局、病院、その他を区別したり、他の方法で確認した属性を利用したポリシー制御が出来る方式を検討する必要がある。

5. まとめ

サービス提供者にXACMLで定義するPDPに相当するものをおくことによりMDBのポリシーやVPN機器の属性を配慮した接続ができ、またサービス利用申請時にHPKIで署名することにより、hcRoleの属性を利用できることを示した。標準化を配慮しXACMLやSAMLのようなXML形式の申請書やポリシーマッチングの標準的形式を検討する必要がある。

6. 謝辞

本研究は情報通信研究機構委託研究:「ネットワーク認証型コンテンツアクセス制御技術の研究開発」において行われた。

参考文献

[1] 第5回 PKIとPMIを融合させる次世代言語XACML.http://www.atmarkit.co.jp/fsecurity/rensai/webserv05/webserv01.html.

SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

VPN 接続許可をポリシー制御可能なダイナミック・オンデマンドVPN

Policy controllable dynamic on-demand VPN to connection permission

喜多 紘一* 鈴木 裕之* 竹田 忠雄† 猪俣 彰浩** 島田 宏†† 有馬 一閣***
Kouichi Kita Hiroyuki Suzuki Tadao Takeda Akihiro Inomata Hiroshi Shimada Kuniharu Arima

あらまし ダイナミック・オンデマンドＶＰＮは２階層 PKI によりルータの接続パラメータをオンラインでダウンロードするのでＮ：ＮのＶＰＮ接続が容易に設定可能である。しかし、多くの対向側通信機器（クライアント側）より VPN 接続を要求されるサーバでは、それぞれの通信機器との VPN 接続の許可を VPN 管理サーバに登録する必要があり、これを安全かつ簡便に行うことが望まれている。本報告ではこの課題を解決する方策を提案している。

クライアント側のルータの登録情報を送付する際に、医療機関の責任者用の HPKI で署名する。サーバはルータが HPKI 付申請のものであれば接続を許可するポリシーをＶＰＮ管理サーバに申請する。VPN 管理サーバはポリシー判定し、サーバへの VPN 接続の許可を登録する。本方式により、医療機関からのアクセスであれば、事前のサーバ側からの接続許可の登録がなくても、オンデマンドで接続許可が登録され、VPN 接続することができ、患者の医療機関に対するフリーアクセスのＶＰＮ環境を実現できる。

キーワード HPKI, ダイナミック・オンデマンド VPN, XACML, SAML, セキュアネットワーク

1 はじめに

1.1 医療情報システムのネットワークの特徴

医療分野におけるネットワークの特徴以下にあげる。

1） 安全な通信
2） 大容量データの高速通信
3） メッシュ型ネットワークの実現と拡張
4） 参加メンバ（利用者、組織、機器）の真正性保証
5） セキュアネットワーク接続に関するコスト削減

1.2 医療情報システムの安全管理に関するガイドライン

医療情報システムの安全管理に関するガイドライン第２版」では、「外部と個人情報を含む医療情報を交換する場合の安全管理に対する最低限のガイドライン」として以下の８項目をあげている。

1） セキュアなネットワーク経路を確保
2） データ送受信の拠点の出入口、使用機器で利用者の必要な単位で相手確認
3） 正規利用者、許可機器への成りすまし防止
4） ルータ機器は安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN 間で送受信が不可となる経路設定
5） 送信元と相手先当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施
6） 医療機関等、通信事業者、システムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社などの組織間で責任分界点、責任の所在を契約書等で明確化
7） リモートメンテナンスを実施する場合は不必要なログインの防止
8） 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認

* 東京工業大学 〒226-8503 横浜市緑区長津田町 4259. Tokyo Institute of Technology, 4259, Nagatsuta-chou, Midori-ku, Yokohama, Kanagawa, 226-8503, Japan.
† (株)NTTPC コミュニケーションズ, NTTPC Comunications
** 富士通 (株), Fujitsu Limited.
†† Heasnt 技術委員会主査, Heasnet Technical Committee chairman
*** (株) NTT データ, NTT DATA CORPORATION

特に1）を満たす対策として、例えばIPSec とIKEを利用することによりセキュアな通信路を確保することがあげている。これを満たすネットワークとしてＩＰレベルでのＶＰＮがあげられる。

また、「外部との医療情報の交換」に関して、以下の５通りの接続形態が記述されている。

1）クローズドなネットワークで接続する場合
　a）専用線で接続されている場合
　b）公衆網で接続されている場合
　c）閉域IP通信網で接続されている場合
2）オープンなネットワークで接続されている場合
　a）回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保した形態でサービス提供する場合
　b）医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合

通常のルータを対で購入してきて、相手先と自分の施設間に設置し、自己責任でパラメータの設定を行うことは、上記2）b）にあたる。

この方式は相手が増えると大変なので、ダイナミック・オンデマンドＶＰＮの普及がHeasnet (Healthcare Information Secure Network Consortium: 保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム)[1] [2]により進められている。

このダイナミック・オンデマンドＶＰＮはこの中の2）a）にあたる形態のネットワークである。通信経路上の脅威の対策のための管理責任の大部分をVPNサービス提供者に委託できる。これにより、医療分野におけるネットワーク要件を満たし、ガイドラインに適合したネットワークを安価で安心できる形で提供することができる。

本報告はこのダイナミック・オンデマンドVPNに更に機能追加を行い、医療分野で使いやすくし、用途を広める為のものである。その説明に先立ってまず、ダイナミック・オンデマンドVPNの理解が重要であるのでその手順を図1を参考に説明する。

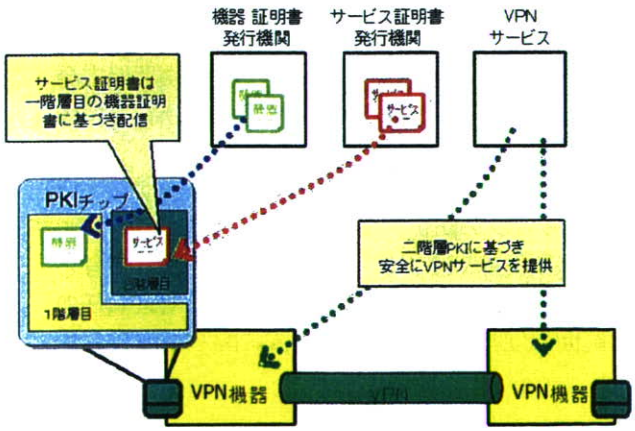

図1　PKI チップによる証明書ダウンロード (Heasnet より引用)

1.3　ダイナミック・オンデマンドVPNの手順

1.3.1.　VPNサービス利用申請

VPN サービス利用申請は電話で言えば電話番号を入手することに当たる。サービス利用者は、機器証明書が搭載されたVPN機器を購入（入手）し、ダイナミック・オンデマンドVPN サービス提供者（以降サービス提供者）に、VPN サービス利用申請をする。サービス提供者は一階層目の PKI で機器証明書により機器の正当性を認証し、VPN サービスの為のサービス証明書をネットワーク経由でVPN機器にダウンロードする。

1.3.2.　接続許可申請

接続許可申請は電話で言えば相手の電話番号の入手

表 1　ダイナミック・オンデマンド VPN とインターネットVPNの比較

比較項目	ダイナミック・オンデマンドVPN	インターネットVPN
機器認証	・VPN 装置に PKI チップを搭載し、電子証明書を搭載し認証可能 ・電子証明書によりｾﾝﾀｰﾄ VPN 装置が認証を行い、機器の成りすましを防止	既存のVPN装置には、認証機能が無いのでオンラインの機器認証は出来ない。
環境設定（使い勝手）	・VPN 装置設置時に機器認証とオンデマンドVPN サービスの認証をインターネット経由で行い、通信が開始できる。(N対Nの接続切替が基本) ・別の相手と新たに通信を行う場合は、聞き認証を元にサービスの為の証明書をネットワークからダウンロードすることにより、通信が開始できる。	VPN 装置設置時に設定した拠点間におけるVPN接続しかできず、新たな相手と接続する場合は、管理者が手動で鍵の設定をする必要がある。 （1対1の接続が基本)
対象者	VPN の構成情報を接続時に配布することと、証明書で保証されたIDで識別しているため、どのインターネットプロバイダーでも適用可能	特定のVPNサービス事業者に限定の可能性がある。

や、相手に自分の電話番号を連絡することにあたる。ダイナミック・オンデマンド VPN の場合、双方から接続をしたい機器を申請、両方から申請（許可）されているものに対してサービス提供者は VPN 接続に必要な「接続情報」を VPN 機器にダウンロードする。

1.3.3. 通信の開始

サービス利用者は通信開始時、通信相手を選択し IKE を行い相手と IP トンネルを形成し、通信を開始する。ダイナミック・オンデマンド VPN は 2 階層 PKI によりルータの接続パラメータをオンラインでダウンロードする。接続相手を変える場合もパラメータをダウンロードすれば良いので N:N の VPN 接続が可能となる。

1.3.4. HPKI 連携によるフリーアクセスの実現

現状のダイナミック・オンデマンド VPN は安全性の観点から、接続元および接続先の双方から接続許可が出されるまで、接続を許可しない。従って患者データが保存された医療関連データベース（以降 MDB）に患者が診療を受けにきた医療機関からアクセスする場合を想定すると、あらかじめ事前に MDB から接続許可のあった医療機関しか MDB と通信できないことになる。いいかえれば、患者はあらかじめ MDB との接続を許可された医療機関へ行かざるをえずフリーアクセスの原則がみたせなくなる。本研究では HPKI を利用してポリシー制御を行い本課題を解決できる方式を提案する。

1.3.5. HPKI について

HPKI は保健医療福祉分野ＰＫＩ（ヘルスケア PKI）の略称である。認定認証業務サービスや公的個人認証サービスが自然人を認証するのに対して、HPKI は医療関連の公的資格すなわち、医師、歯科医師、薬剤師などの属性を自然人に付加して認証する。また、医療施設の管理者も認証することが出来る。公開鍵証明書の hcRole の項目により証明する。証明書ポリシーが厚生労働省より出されている。

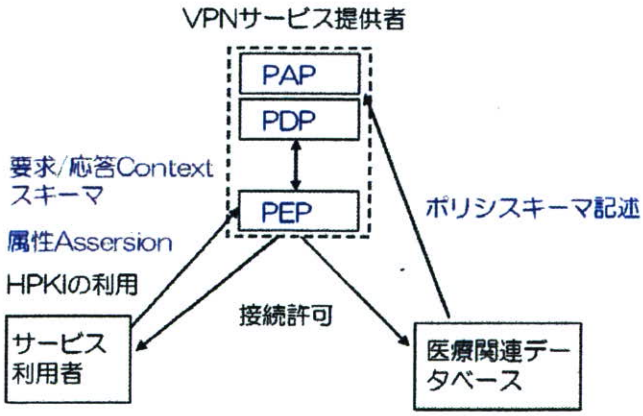

図２　接続許可ポリシー制御

2　方法

2.1　HPKI 署名付サービス利用申請書

医療機関が VPN サービス利用申請として VPN 機器の登録情報を VPN サービス提供者に送付する際、申請書に医療機関の責任者用の HPKI で署名する。MDB は接続申請時に接続申請する機器が HPKI 付申請のものであれば接続を許可することを VPN サービス提供者に申請する。VPN サービス提供者はあらかじめ HPKI 署名付申請で医療機関であることを登録した VPN 機器からの接続申請かを判定し、MDB への接続を許可する。この場合、接続の合意は MDB のポリシーと一致することにより事前確認が双方で取られているものとみなす。このポリシー制御の考え方は XACML の概念に類似している。

2.2　XACML およびＳＡＭＬの概念の利用

XACML は PDP (Policy Decision Point)、PEP (Policy Enforcement Point) および PAP (Policy Administration Point) のキープレーヤを定義している。[3]

ダイナミック・オンデマンド VPN では PEP は接続許申請に対し接続情報の VPN 機器への配布点にあたる。PDP はポリシーに基づく接続許可の判断する点にあたる。PDP は PAP のポリシーに基づき判断を行う。

XACML は 3 つの Context を定めている。PAP から PDP に示すルールやポリシーを記述するための「XML スキーマ」、PEP がアクセス要求者の属性情報を記述して PDP に提示する「要求 Context」および PDP が PEP に返す認可決定の「応答 Context のスキーマ」である。

「ポリシーを記述するスキーマ」は MDB の接続許可申請時に「MDB に対して接続許可申請する VPN 機器が HPKI 付申請のものであれば接続を許可する」ポリシーをＶＰＮサービス提供者に申請するときの構文の考え方に使用できる。

また、SAML では「認証オーソリティ」と「属性オーソリティ」が Assersion を Response として応答するときにオーソリティの署名つきで応答する。これは「VPN サービス利用申請時、申請書に医療機関の責任者用の HPKI で署名する」時の構文の考え方に利用できる。ただし、PDP が署名の属性も利用するところが異なっている。

2.3　プロトタイプの実験

プロとタイプの作成は通常のダイナミック・オンデマンド VPN にポリシー制御部分を付加して行った。まず通常の VPN 機器登録後、MDB は接続を申請してくるクライアントがどのような属性を持っていれば接続を許可するかのポリシーをＸＭＬ形式で作成し、これに署名をおこなってサービス提供者に申請する。今回は医療機関とか薬局であれば接続するなどのポリシーを仮定して

行った。クライアント側も医療機関用のＨＰＫＩ証明書に対応する秘密鍵で自己の機関の属性申請書に署名を行う。HPKI 証明書は hcRole で医療機関か薬局かを区別することが出来る。これによりサービス提供者はそのクライアントの属性を知ることができる。クライアントが MDB にアクセスする場合は MDB を指示するとサービス提供者はポリシーマッピングを行い、ポリシーに合っていれば、接続許可を VPN 機器に出すこととした。

クライアントと MDB 間の通信を開始し相互の接続の確認を行った。

3　結果

本方式により、医療機関からのアクセスであれば、事前の MDB 側からの個別接続許可がなくても、接続を可能とすることができ、患者の医療機関に対するフリーアクセスの環境を実現でき、医療関連施設間のネットワーク基盤すなわち医療ドメインネットワークを形成することができることを確認した。

4　考察

医療機関というだけで MDB 側が接続を許可するのはダイナミック・オンデマンド VPN のセキュリティポリシーの制御として十分ではないとの考え方もある。その為には hcRole を使って、例えば薬局、病院、その他を区別したり、他の方法で確認した属性を利用したポリシー制御が出来る方式を検討している。

現在基礎検討が進められている、電子私書箱構想において、健診機関等から健康・医療情報を電子私書箱へ提供するネットワークは提供者に何らかの制限を与えるとすると本提案が使用可能である。また、電子私書箱のデータを医療機関側で参照する場合もアクセスするネットワークはフリーアクセスの必要があり、本研究で提案のネットワーク機能が適している。

また、今回は HPKI を利用したが社会労務士等資格を証明する公開鍵証明書やその他セキュアな識別子を利用してポリシー制御することが可能である。

また、医療機関であることの申請はサービス利用申請時でも接続許可申請時に行っても良い。

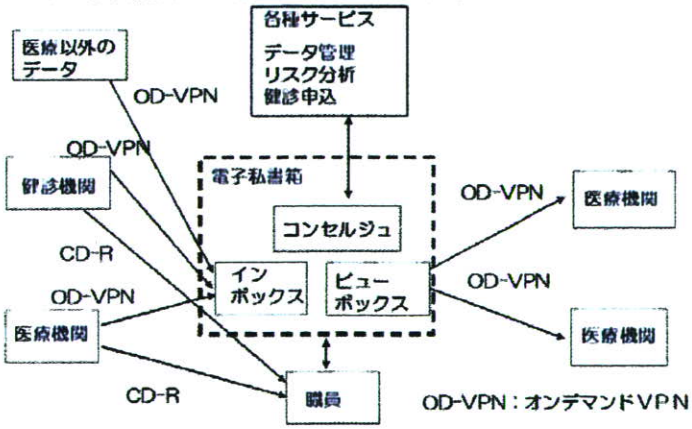

図３　電子私書箱構想による個人健康情報参照システム

5　まとめ

サービス提供者に XACML で定義する PDP に相当するポリシー制御機構をおくことにより MDB のポリシーや VPN 機器の属性を配慮した接続ができ、またサービス利用申請時または接続許可申請時に HPKI で署名することにより、hcRole の属性を利用できることを示した。標準化を配慮し XACML や SAML のようなＸＭＬ形式の申請書やポリシーマッチングの標準的形式を検討する必要がある。

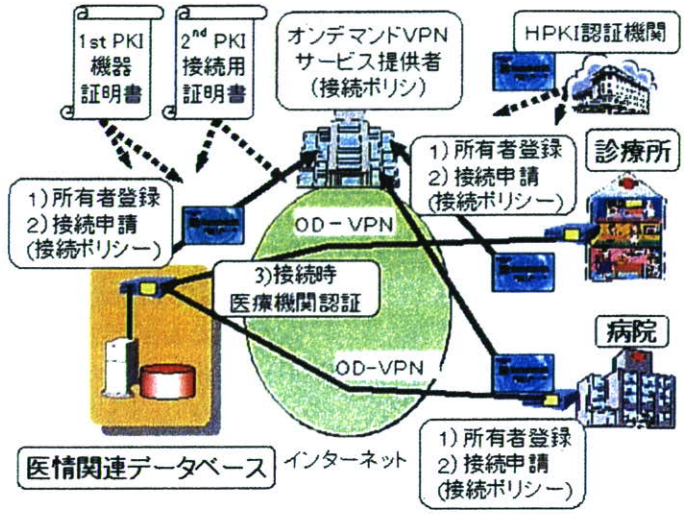

図４　ポリシー制御可能なダイナミック・オンデマンドVPN

謝辞

HPKI による機関認証部分の基礎技術開発は情報通信研究機構委託研究:「ネットワーク認証型コンテンツアクセス制御技術の研究開発」において行われた。また、電子私書箱の医療応用構想部分は文部科学省科学技術振興調整費による支援を受けている。

参考文献

[1] Heasnet（Healthcare Information Secure Network Consortium: 保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム),
http://www.heasnet.jp/index_J.htm

[2] 高橋 成文, 東川 敦紀, 山本 修一郎, 小尾 高史, 谷内田 益善, 大山 永昭,「2 階層 PKI を用いたオンデマンド VPN システム」, 情報処理学会論文誌, Vol.46, No.5(20050515) pp. 1129-1136, 情報処理学会, 2005

[3] 鈴木 優一,「第 5 回 PKI と PMI を融合させる次世代言語 XACM」
http://www.atmarkit.co.jp/fsecurity/rensai/webserv05/webserv01.html, 2002

個人情報の利活用を可能とするサービス基盤に関する研究

Study on Service Infrastructure for Utilization of Personal Information

岡野翔[*1] 鈴木裕之[*1,2] 小尾高史[*2,3] 山口雅浩[*1,2] 谷内田益義[*2] 大山永昭[*1,2] 喜多紘一[*2]
Sho Okano, Hiroyuki Suzuki, Takashi Obi, Masahiro Yamaguchi, Masuyoshi Yachida, Nagaaki Ohyama, Kouichi Kita
[1] 東京工業大学像情報工学研究施設
Imaging Science and Engineering Laboratory, Tokyo Institute of Technology
[2] 東京工業大学統合研究院
Integrated Research Institute, Tokyo Institute of Technology
[3] 東京工業大学総合理工学研究科
Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology

1. はじめに

現在，医療や年金などの個人の情報は機関ごとに個別に管理されており，本人はどのような情報が管理されているのかを知ることができないため様々な問題が生じている．そのため，各々の機関で管理されていた情報を本人が自らのものとして一元的に管理・統合し，利活用できる社会の構築が望まれている[1]．ここで個人の情報を取り扱う際には，本人の意思に基づいて情報を安全に利活用できることが重要であり，また個人ごとの好みに応じた利活用の仕方ができることが求められる．本研究では，各機関から開示された個人の情報を利用者が安全かつ柔軟に利活用可能なサービス基盤の実現を目的とし，SaaS(Software as a Service)モデルに仮想化技術を適用して，SOA(Service Oriented Architecture：サービス指向アーキテクチャ)と組み合わせたサービス提供モデルを提案する．

2. 課題

本研究では，各機関から利用者へ開示された情報は一元的に保管され，その情報を基に利用者が自由に利活用するサービス基盤を対象とする．このような仕組みは，ネットワーク経由でソフトウェアの機能をサービスとして提供/利用する SaaS モデルを適用することが有効であると考えられるが，サーバに大量のデータが一元的に保管されるため，情報漏えいのリスクがある．したがって，複数の利用者でサーバを共有しても情報を安全に保管し，本人の意思に基づいて利活用できる仕組みが必要である．また，情報の利活用の仕方については，利用者の好みによって多様なニーズが存在すると考えられ，サービス提供者が予め用意したサービスだけでは，必ずしも利用者のニーズを満たすとは限らない．そのため，利用者が自由に好みに応じたサービスを利用できる必要がある．

3. 解決方法

サービス基盤を提供する事業者（直接サービス提供者）が所有するサーバで個人の情報を安全に保管し，利用者の意思に基づいた情報の利活用を可能とするために，セキュア VM(Virtual Machine：仮想マシン)を用いてサーバ上に仮想マシンを配置し，本人のみがアクセスできる隔離された実行環境を提供する．これによって複数の利用者でサーバを共有しても，各利用者のデータやアプリケーションの安全性を確保することができ，利用者は仮想マシン環境で好みに応じてアプリケーションをインストールしてサービスを利用することができる．また，仮想マシンで利用するアプリケーションは SOA に基づきネットワークを介して外部のサービスを柔軟に組み合わせることによって構築する．そのため，各サービスには必要最小限のデータのみが提供されるとともに，利用者の好みに柔軟に対応可能な利活用のサービスを提供することができる．[Fig.1]

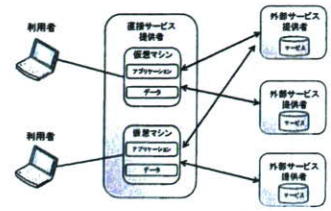

Fig.1 システム構成

4. 実験システム

健康増進を目的とした健康管理支援サービスを想定し，提案するサービス提供モデルを基に実験システムを構築した．医療機関から開示された健康診断データは，各利用者の仮想マシンに保管されており，アプリケーションはネットワークを介して外部のサービスを連携させて，データ分析結果を表示する．サービスの連携には Web サービスの技術を用いた．Fig.2 に 2 人の利用者が本サービスを利用した際のアプリケーションの実行画面例を示す．

(a) 利用者 A の画面　(b) 利用者 B の画面

Fig.2 健康診断データとデータ分析結果の画面例

5. まとめ

本研究では，個人情報の利活用を可能とするサービス基盤を実現するために，セキュア VM によってサーバ上に仮想マシンを配置し，SOA に基づいて外部のサービスを連携させてアプリケーションを構築することで実現できることを示した．また，実験システムを構築し，提案手法の有効性を確認した．

参考文献

[1] IT 新改革戦略 政策パッケージ
(http://www.kantei.go.jp/jp/singi/it2/)
[2] NICSS 要件書 第 1 版
次世代 IC カードシステム研究会

「電子政府・電子自治体推進フォーラム」基調講演

去る10月17日（火）、東京都千代田区永田町のキャピトル東急ホテルにおいて開催された「電子政府・電子自治体推進フォーラム」（本誌12月号（No.409）参照）の基調講演について、当日の講演内容をもとに、大山永昭東京工業大学教授の加筆・修正を経て、以下のとおり掲載いたします。

なお、本講演の当日資料及び基調講演後に行われたパネルディスカッションの概要については、日行連HP上（当日資料：「会員ページ」→「各種資料」、ディスカッション概要：「トピックス」一覧）に掲載しておりますので、併せてご参照願います。

「電子政府・電子自治体の実現について」

東京工業大学教授　大山　永昭

どうも皆さんこんにちは。今、紹介いただきました東工大の大山です。

これから30分ほどの時間を使って、基調講演を行います。この講演は、後のパネルディスカッションにつなぐための話題提供になります。

30分ほどの講演なので、表面的な話になりますが、まず、IT新改革戦略の基本的な考え方について、次に電子政府と医療の情報化に関する類似点と相違点の比較を、そして電子政府の現状と課題、医療分野の課題と社会保障サービスに関して、最後に住基カード2.0あるいは電子的な身分証明、eIDの導入について説明します。

IT新改革戦略の基本的な考え方

まず、新改革戦略の基本的な考え方です。ご案内のとおり、平成18年の１月19日に決定、公表されています。目標は2010年です。私自身、新改革戦略の起草では主に医療と電子政府を担当してきました。基本的な理念としては、構造改革による飛躍という話が出ています。中でも社会的なジレンマの解消支援に焦点が当てられています。

例えば少子・高齢化に伴うさまざまな社会的なジレンマがあります。言うまでもなく、高齢化というのは寿命が伸びているわけですから、これは喜ぶべきことですが、一方では、少子化によって、いわゆる労働者人口が減少します。したがって、従来の年金や医療保険のモデルがなかなかうまく成り立たないことなどがジレンマになっています。そのため、ICTが梃となってこういう社会的なジレンマの解消に貢献することが重要視されています。

他には、利用者・生活者の視点、これは当然のことですが、さらに、国際競争力の強化、国際貢献といったようなことがうたわれています。

戦略を議論するときの基本的な認識として、社会的な課題を大きく取り上げたので、その観点から短期的すなわち二、三年で何をすべきかが検討されました。その結果、まずはICTを用いたビジネス・プロセス・リエンジニアリングすなわち業務プロセスの改善等を行うべきとの結論に達しました。

特に、現在の電子政府の状況を見ると、各府省の中では、制度ごと、あるいは業務ごとにシステムがつくられていますが、これらはそれぞれ独立していて、無駄なリソースが散見されます。分散処理が悪いというわけではありませんが、残念ながら横ぐしがありません。そのため、各府省ではどのようなシステムを使っているのかを調査し、それらのシステム全体を最適化するために、プログラム・マネジメント・オフィス（PMO）を設置すべきとしました。

さらに、中央政府全体では、府省共通業務を含めたガバメントのPMOの設置を決めました。これらは業務プロセスの見直しと併せて、コストダウンによる財政の健全化につながると期待しています。スライドには直接書いてありませんが、実は、このコストダウンされた費用の一部を、次のIT投資にどう振り向けるかというのも大事な観点と考えています。

これはあくまで短期的な話で、やはり5年先を見ると、自ら考える知的な社会の実現が極めて重要です。そのためには、分かりやすくシンプルで、さらに透明な制度構築が必要であるとしています。なぜならば、逆のことを考えると分かりやすいのですが、現在の制度の中には複雑でよく分からないものが多くあるからです。

例えば、行政書士の皆様方は専門家ですから、皆さんに申し上げるのはちょっと変かもしれませんが、例えば年金の制度がどうなっているか、医療保険制度がどうなっているか、多くの方はよく分からないと思います。先日も私の先輩といろいろ話していたら、近々、年金をもらうようになるので、その金額を聞きに行ったそうです。すると、ある金額が提示され、こんなものかと思ったそうです。

ところがその後、別の通知が来て、前の額は間違っていましたと知らされたそうです。年金の給付額は、しっかりとしたルールのもとで算出されるものですから、誰が計算しても同じになるはずです。裁定をするための何らかの裁量権があるのかなとの疑念を持ってしまいます。このことは言い方を変えると不信感につながっていく場合があるわけです。このような不信感を払拭するためには、誰にでも分かるように透明性をあげなければなりません。

分かりやすくシンプルで、さらに透明な制度になれば、システム全体を最適化することも可能になります。当然のことながら、国と地方自治体がつながるシステムのグランドデザインを作ることが、今回の戦略の第一歩であると考えています。

自ら考える知的な社会では、さまざまな社会的な問題や課題、あるいは自分や家族の生活、もちろん老後も含めてですが、これらのことを考えられる環境が必要です。そしてそのためには、本人に対して情報を開示することが不可欠です。今までは、行政が持つ情報の公開が原則になっていますが、今度は個人情報についても開示する必要があるということです。これがこの後の話になる住基カードのような厳格な本人確認を必要とする一つの理由になります。具体的な例としてはレセプトやカルテの開示があげられます。

中央政府全体について言えば、現在行われているシステムの最適化は個別システムの最適化なので、今後は全体最適へ向かうことが必要です。その結果、既存システムの刷新・統合・廃止といったものが行われることになると思います。

さらに社会保険庁の例がよく出ますが、ITガバナンスが社会保険庁側になくて、システムを受けていた企業側にあったために現在のような問題が起きたように、政府側のITガバナンスの確立が不可欠です。このことに関しては、この後、中井川さん（パネリスト）のほうからお話があるのではないかと思います。

またPDCA（計画・実行・評価・改善）については、何がどこまで進んでいるのかを評価する成果指標が必要です。この観点から、今回は、行政分野とそれ以外の公的な分野に分けています。このように分けたのは、行政分野では官のみがサービス提供を行っているのに対し、その他の公的な分野では官及び民がサービス提供を

行っているからです。

もちろん、どちらの分野にも公的資金が入っています。その結果、電子政府に関する成果指標は、当然のことながら利用率の向上を目的としたPDCAの活用が出てきます。それに対して後者、すなわち医療や教育が代表格ですが、これらに対してはコンピューターシステムを含めた事務経費の削減を求めることになりました。そしてこの考え方から、医療分野、独立行政法人等も対象にしました。今回のIT新改革戦略の中で最初に比較的大きく報道されたレセプトの完全オンライン化は、この一律事務経費の削減という観点からお願いしたということです。

電子政府と医療分野の情報化との類似点と相違点

電子政府と医療分野の情報化は非常に似ていますが、その類似点と相違点をまとめてみます。

似ているところは公金が投入されていて、費用の総額抑制が社会的背景から強く求められているということです。これに反して、実際にその責を負っている方の多くは残念ながらあまり気になさっていないのではないかと思います。要するに、お金はどこかからか来るものと思っている方が多いという印象を持ちます。そして、業務・システムの最適化が有効に機能する分野であると思います。これは裏を返すと、それだけ現状システムには無駄があるということですから、早急に対応すべきです。さらに、どちらの分野でも厳密な本人確認を必要とするものが多くあるということです。もちろん簡単なものもありますが、医療および電子政府においては、本人確認および本人の意思確認が非常に重要になっています。

一方相違点としては、電子政府が進んでいるのに対して、医療の情報化は遅れていることがあげられます。その最大の理由は、医療では、サービス提供が官・民の両方によって行われていることから、なかなか有効策が出なかったことがあげられます。

電子政府の実現手順を示します。このことはこれまで何回も説明しているように、まずは役所内部の情報化です。次に、行政機関の間をネットワーク化します。ここで中央政府においては、霞が関WANとGPKI、すなわち安全なネットワークと電子署名の２つを必要としました。地方自治体ではLGWANとLGPKIの２つがやはり必要でした。３番目がサイバー空間への拡張で、これは、誰でも入れるインターネットのようなネットワークを経由して行政機関にアクセスし、双方向の通信を行うということです。ご案内のとおり、96%以上がオンライン化されていることからも構築はほぼ終了して、今後は安定実稼働へ進むことになります。もちろん使い勝手等で未だ不十分なものがあるのは重々承知していますが、だからこそシステムを改善し、利用率を向上することになります。さらに全体の最適化へもっていくのが、今後の５年間にやるべきことだろうと思っています。

今のことを念頭において医療分野の情報化を眺めてみると、やはり同じように３つのステップになることが分かります。第１ステップは、医療機関の情報化です。電子カルテ、会計・事務システム等の導入ということになります。電子カルテは、ご案内のとおり、まだ20%ほどしか普及していません。会計・事務システムは、それに比べてかなり大きく90%以上の導入が既になされていますが、どちらにしろ医療の情報化では第１フェーズが終わっていないということです。

第２フェーズは、医療機関のネットワーク化で、そのためには安全なネットワークとヘルスケアのPKIが必要になります。HPKIは医師等の医療従事者の役職を含めた電子署名です。ちょうど行政書士さんたちのPKIに入っているのと同じような仕掛けです。HPKIは、今年から厚生労働省が制度的にも正式に実施する準備に入っており、間もなく開始されると思います。一方、ネットワーク化に関しては、医療関連機関は全国に22万組織ほどあります。これらの機関をどのように接続するかということが大きな課題になります。自治体よりもはるかに多いの

で、専用回線を用いるのか、他の方法を使うのか等に関して、ネットワークの利用形態を踏まえた検討が必要です。そもそも個人の患者さんの情報が流れますが、医療機関ならばどこでも個人の医療情報を見ていいよとはならないと私は思います。言い換えれば、お医者さんや患者さんの移動に伴って、必要なときに必要な相手と安全に通信を行えるようにすることが大切であると考えます。このような環境を実現するために、Dynamic、すなわち接続先が変わるという意味のDynamicで、要求があるときにつながるOn－demandをつけたＶＰＮという新しい技術を開発しました。

第３フェーズはサイバー空間の話になります。具体的には例えばネット経由の医療相談等で、本人確認のために公的個人認証サービス等を利用することになります。この公的個人認証サービスによって患者さんを、HPKIによって医療従事者の方を確認できます。こうすることでお互いに相手確認をした上で、安心して医療相談等ができるようになります。

以上のことから、新政略では第２フェーズ以降を主にしています。もちろん電子カルテの普及は引き続き努力をしなければならないところでありますが、現実の利用形態を考えると、電子カルテよりは退院時のサマリー等の電子化などの重要性が高いと思われます。

電子政府の現状と課題

これまでの取り組みについては、既に多くの方がご存じと思いますが、書面等、法令等で電子化の妨げとなる文言などの改正や電子署名法の制定、e－文書法の制定など、必要な環境整備がほぼ完了しています。KWAN、GPKI、LGWAN、LGPKIの構築があって、現在は公文書の交換が電子的にできるようになっています。さらには、住基ネットの構築、住基カード、公的個人認証サービスの３つの基盤を整備して、サイバー空間へ、すなわち第３フェーズまで入れるように環境は整のっているということです。

以上をまとめると、これまでの取り組みのところでは、2005年度末までに構築をほぼ終了し、オンライン化率96%以上になりました。また、CIO及びCIO補佐官の設置、レガシーシステムの刷新、業務・システムの最適化計画の策定と作業を行っているというのが現状で、年間のシステム運用費は中央政府だけで約１兆円と言われていますが、これが8,700億円以下に削減できる見通しを得ています。損益分岐点はまだ数年先にもちろんなりますが、しっかりとコストを下げる道を見つけてきたというのが現状です。

最大の問題は、利用率が0.6%、最近0.7という統計もありますが、この利用率の低さです。そのためにはインセンティブの付与、具体的には所得税、法人税等電子申告控除制度の導入などのいろいろな対策が検討されています。

今後、具体化された対応策が出てくると思いますが、中でも、団塊の世代の方に対するリタイヤメントポータルが必要と思います。これは御案内のとおり、来年から2010年までに約800万人の方が退職しますが、この方たちが新たな生活に移るときには、健康保険組合や年金の変更などさまざまな手続が必要になります。これらの手続き等に団塊の世代の方たちがうまく対応いただけるようにリタイヤメントのためのポータルをつくるのが効果的ではないかということです。

一方中央政府においては、ITガバナンスの極端な不足が大きな問題です。いわゆる丸投げ体質からの脱却をしなければなりません。そのためには人材育成そのものが大きな課題になると思います。

それから、現状では個別システムの最適化が行われていますが、全体最適にはなっていません。そのためにGPMO、PMO、電子政府評価委員会を設置し、PDCAサイクルをドライブしています。さらに、住基カード、公的個人認証サービスの普及が進んでいません。これに関しては社会保障を含めたICカード、仮称で新行政カードと呼びますが、このカードの発行に関する検討がIT室で行われています。社会保障とい

う意味では、年金、雇用保険、医療保険、介護保険、すべてのものが対象になります。これはリタイヤメントポータルにも直接つながります。

さらにすこし先を考えると、災害に強いシステムにすることが不可欠です。このためにはバックアップシステムの設計と構築が必要ですが、現在のように全体最適化もせずにすべてのシステムをバックアップしたら大変な費用になります。言うまでもなく、それは無理な話です。早急に全体最適の設計を行ない、できているところからバックアップをつくることが必要です。それまでは、大きな災害が無いことを祈るのみになります。全体最適化の一環として考えるべきものとしては、先ほど申し上げたように、制度別、あるいは業務別のシステムを国民中心のシステムに変更することが有効です。現状では、何か新しい業務ができると、新たな業務システムができます。これは非常におかしな話で、国民を中心に考えれば、システムが増えるわけではなく、ソフトウエアが一個増えるだけのはずです。このような観点から、最近では社会保障番号や個人口座開設の議論がされています。さらに、IT投資の原資不足も指摘されているところです。

住基ネット、住基カードから学んだこととして、先ほど言った業務、あるいは制度別にシステムができているということ等を含めて説明します。ご案内のとおり、住基カードの普及は残念ながらおくれています。これは費用対効果が十分でないことが主たる原因と考えます。皆さん方の中にも住基カードをお持ちの方がいらっしゃると思いますが、その方々には心から感謝いたします。ただ、何に使っていますかというのはあまり聞けない状況ではないかと思います。身分証明書になるのを非常にうれしく思ったこともありますが、本来の目的である電子空間における本人確認のための仕掛けにはなかなかつながっていません。この原因の一つは、最近、私自身経験したことですが、省庁の縦割りによる弊害であるとあえて指摘したいと思います。

というのは、年金の現況確認の廃止に絡む話です。ご存じのとおり、年に一回誕生日の前になると、年金をもらっている方たちに元気ですかというはがきが送られます。生存証明をもらって送り返すのが現況確認ですが、ご多分にもれず、年金の現況確認システムというのがあります。はがきを打ち出すためのシステムがあって、それを郵送して、年金受給者の方々が自ら生存証明をもらって返送します。その後、その結果に従ってシステムに再入力をします。この一連の作業が、住基ネットを使うことで無くすことができます。

私も委員の一人ですが、この内容が社会保険庁の改革推進委員会で説明されたときに、私から見ると、住基ネットを使えばできるのは当たり前と思っていたのですが、ほかの委員の方から住基ネットに価値があるのですねというお話をいただきました。住基ネットの構築を考えていたときは、当たり前と思っていましたが、世の中にはその可能性が伝わっていなかったことに気づきました。言い方を変えると、住基ネット導入の効果の例として、われわれが言っていた引っ越し手続きの軽減などだけでは、十分ではなかったということです。現況確認の廃止は、2,500万人以上の方々が対象であり、その方たちの手間とともに、社会保険庁業務の軽減にもなるので、住基ネットの利用効果を明確にすることができたのです。

これはつくる省と使う省が違う場合の苦しみの例であると思います。その意味では、政府全体としての方針決定とメリットの明確化を図るべきであると、最近、強く思います。そのためには、政府全体に横串を通す、あるいは全省庁に対して傘をかぶせることが必要です。現在の傘である内閣官房は、調整することはできますが、他省庁への命令権限や予算執行権限はありません。そのため、どうしてもうまく機能しない場合が多々あります。早急に、改善することが必要でしょう。

悪いことばかり言っているように聞こえると申しわけないのですが、もちろん良いこともあ

ります。このような課題に気づいた人が何人も増えたということです。今までは全く気にしなかったのですが、改善しなければならないと考えている方が多くいることは、非常に大きな励みになると同時に、必ずやりあげることができると信じています。

医療分野の課題

医療分野の課題ですが、現状は、先ほど言いましたように、情報化はあまり進んでいません。戦略策定時に医療の情報化の状況確認を行ったところ、最初に出た言葉が医療の近代化が必要とのことでした。情報化をする前に近代化が要るという話でしたが、だからこそICTを梃にしたいのです。言うまでもなく、医療分野のIT化は難しい面が沢山あるので、確実に進めなければなりません。なぜIT化が必要かといえば、先に述べた社会的なジレンマがあるからです。具体的には、例えば財政の余力と国民の満足があれば、医療費の増大は許容すべきか、ということです。私はイエスであると思っています。言い方を変えれば、ではなぜ今、問題が起きるのかといったら、財政の余力がないからです。

また医療費等が国民に不透明であることも大きな問題です。これらの問題を解決するには、本人に関する医療関連情報の開示が要ると思います。他にも、保険診療と自由診療のいわゆる混合診療を全面的に認めるべきかという話があります。

また、現在の日本では、患者さんは医療機関を自由に選べます。しかしながら御案内のとおり、保険の制度によっては、医療機関を指定している国もあります。どっちが良いのでしょうか。さらに、効率化、医療費の適正化はないのかということがあります。これはもう明らかで、絶対に道はあると思います。それから、医療過誤等を防止するためのICTの利用方法はないのでしょうか。これも当然あると思います。では、なぜ使わないのか、なぜ普及しないのでしょうか。お医者さんや看護婦さんをはじめとする医療従事者の方たちは、日々ものすごく大変な思いをして忙しく働いています。あの様な環境で人的なミスが起きないはずはないと思います。そこに対してICTが使えないのは、財政的な問題か、人手不足か、必ずどこかに本質的な問題があるはずです。このようなジレンマの解決に対して、ICTが幾らかでも資することができないのかが、医療分野のIT推進、利用促進を考えるときの大事な原点であると思います。

今回の戦略にレセプトのオンライン化を取り上げたのは、事務経費の削減を目的にしたからです。現在、レセプトと呼ばれている医療費の請求は年間16億件あります。このうちの900万件が返戻といって保険組合から医療機関へ差し戻しになります。その中の半分は資格が確認できないことに起因しています。

また900万件のうちの4割、360万件ほどが、保険証番号等の転記ミスに起因しています。現在は、総数で16億件、紙にして30億枚以上が使われていますが、全部人手で動かしています。請求内容のチェックも全部人手です。これを電子化して経費が下がらないはずはないというのがわれわれの予測です。もちろん、オンライン化すると大変ですよと言う人もいます。どちらが正しいかは、今後明らかになると思いますが、少なくとも今の金融機関が昔のように紙に戻ることは考えられません。それなのになぜ医療だけは紙から電子に変えると経費が高くなるのかは不明です。

また、個人の健康情報等、生涯を通じて利活用できることを取り上げています。われわれの体のぐあいは徐々に変化します。そのため生活習慣病等では、長い期間の健康状態を見てはじめて傾向がわかります。このような情報をうまく予防医療につなぐために活用することを考えています。

3番目は、効果的なコミュニケーションで、最初の2つが医師対医師です。具体的には山間僻地・離島における遠隔医療や高度専門医療における遠隔サービス等です。3つ目が医師対患者になります。ご存知のように、2011年に我が国では地上波のアナログ放送が停波されて、地

上デジタル放送にかわる予定ですが、この受像機はデジタルなので、まさしくサイバースペースへの入り口になる可能性を持っています。ですから、このテレビ受像機を使って、さらに、その中にある双方向通信、簡単に言うとインターネットの口がついているということでありますが、これを使って受信前医療提供サービスの効果検証を行いましょうということです。特に、救急搬送依頼時では、救急車が着くまでに現場にいる方々を支援するというものです。

また、小児救急における医療相談サービスも有効ではないかと考えています。ご存知のように、おじいちゃん、おばあちゃんが一緒に住んでいたころと違って、現在は核家族化されています。そのため、経験の無い若いお母さんやお父さんは、急に赤ちゃんが発熱するとパニックになります。このような場合に、親御さんに対して適切に支援しようとするものです。最近の消防庁のポスターには、驚くことに「救急車はタクシーではありません」と書いてあります。これは大変なことで、それだけ救急車を使っている方が多いことを表わしています。もちろん今の制度では、呼ばれたら行かなければならないのですが、やはり適切な使い方をしていただきたいということです。具体的にはＴＶにデジカメなどを接続すればよいのです。これでお医者さんと相談ができるようなれば、役に立つのではないかと思います。当然このときには、必要に応じて、ここは、ネットワークの安全性を確保することが必要になります。

このときに、相談に乗ってくれる方が医師かどうかを確認することが必要になります。将来的には医療行為に当たるものもサービスされると考えると、この場合には医師であることを確認する必要性が生じ、ここで先ほど言ったＨＰＫＩがまた出てきます。患者さん側についても同じことで、相手がどこの誰かを間違えたらとんでもない事になります。ここで住基カードと公的個人認証サービスが再び登場します。幸いなことに地上デジタルの受像機をお持ちの方は、Ｂ－CASと呼ばれるカードが入っているのをご存知と思います。ここに住基カードを差すことで厳格な本人確認ができるというのはどうでしょうか。

さらには、インフラの整備や情報化推進体制の整備とグランドデザインの策定が必要と書いてあります。

社会保障サービスの関連について、社会的な現状と予想を簡単に説明します。まず、少子・高齢社会なることを考えると、少子化は長期的には労働者人口の減少を招きます。高齢化は当然のことながら社会保障費の増大につながります。このことから、財源不足になることは明らかです。だからこそ国民の満足と財源のバランス確保が必要になるのです。この状況を加速したのが、最近起きている社会保険庁の不祥事です。この不祥事は国民の不信を招き、年金の未払いが起きて、従来モデルが崩壊しつつあります。このような悪循環ができてしまいました。それぞれの課題、すなわち、不信感を回復するため、年金の未払いを防止するためなどについては、個別の対策を講じていますが、現状ではまだ不十分ということです。

問題の本質は何かと言えば、最初に申し上げたように、制度が複雑でよく分からないために、国民が興味を失っていることです。年金、うーん、払ったほうがいいのか、払わないほうがいいのかもよく分からなくなっています。よく言う話ですが、ルールが複雑なゲームのファンは少ないということで、これはまさしく興味を失わせる最大の原因になっています。さらには、不公平に見えているから不信感が募る結果になります。ネガティブループから脱却するためには、本人に関する情報の開示をして自分の状況が分かるようにすること、すなわち、例えば年金を掛けるほうが、貯金より得であることを明確にするべきです。そもそも税金が投入されているのですから損にならないはずです。もっとも早く亡くなってしまうと残念ながら戻ってきませんので、ちょっとそこは違いますが、もともと社会保障の精神が世代を超えた助け合いにあるはずです。この意味で、社会保障の個人ア

カウントを開設するということで、出入りを見せるというのも一つの考え方なので、最近の話題になっているのだろうと思います。このアカウントに対するアクセスは、安全かつ確実でなければならないので、電子的な身分証明書が必要になるのです。

個人または家族でアカウントをつくると考えると、社会保障に係わる電子的な記録簿です。関連する各種情報の提供、例えば納付、受診等の記録、健康保険の種別と資格などさまざまなものが扱われます。さらには、本人あるいは家族に開示された情報が入ってくるので、ＩＣカード等を用いてアクセスコントロールをかけて、十分な安全性を確保します。この辺のやり方は、技術的には問題ないと思います。現在、年金の納付記録等に不備があることが指摘されていますが、こういったものも本人に開示することにより確認･訂正等ができるようになります。こうなれば、社会保険庁のデータベースもオープン化することができます。なぜ今できないかというと、データベースは高速な検索を可能にするために、一般的に記録されているデータはオブジェクトではなく、特殊な構造をしていること、およびデータの完全性が確認できていないことが主たる原因です。

一方、このアカウントに送られるデータは、オブジェクト化され、なおかつ検索スピードを要求しないので、時間をかけてデータをきれいにすることが出来ます。したがって、確認されたデータから新たなデータベースに移行させることで、結果として、データベースの刷新が出来ると考えられます。必要となる容量を試算すると、例えば１アカウント10メガで、5,000万アカウント、これは世帯数にあたりますが、これですと総容量は500テラバイトになります。今の技術では、それほど大変なことではありません。

最近、社会保障番号導入の議論がされており、個人を特定するための番号といっています。これはIdentifierなので、他に特定できるものがあれば、必ずしも番号である必要はありません。社会保障番号の付番対象者が、住基ネットに登録されている日本の方と社会保障を受けている外国人の方になること、および両者には異なる番号体系があることなどを考えると、新たな番号をつける必要性は低いと思われます。もちろん、外国人登録が変わるという法務省の動きも考慮すべきですが、住民票コードの利用制限があることなどを考えると、この社会保障番号にはどちらにしろ、法令による利用範囲と利用制限の明確化や社会の受容性に対する十分な配慮が不可欠です。

一方、アカウント番号は、どちらにしても、必要になります。もともとアカウントは、説明責任を意味するアカウンタビリティにつながるので、アカウントをつくるというのは、国が社会保障に関して国民に対してアカウンタビリティを確保するためのものというように考えることができます。

スライドには他にもいろいろ書いてありますが、時間の関係もありますので、説明を省略いたします。

eID（住基カード2.0）の導入に関して

次に住基カード2.0について紹介します。先程から説明していますように、機微な個人情報を開示するためには、何らかの本人確認手段が不可欠です。この本人確認は対面で行う場合と電子空間すなわちネットワーク経由の場合が考えられます。この目的に合うものは、一般的にeIDと呼ばれています。

eIDには３つの機能が必要と言われています。すなわち本人を特定して、その特定情報が正しいことが保証され、さらに本人の意思を確認するものです。これらはIAS機能と呼ばれ、ヨーロッパ、アメリカ、アジアの世界中の国々でほぼ同じ考え方になっています。

eIDを使った保険証の例を説明します。先ず新行政カードの発行手順の案を紹介します。カードの交付を受ける方は住基カードと同じように市町村に行って申請すると、発行センターからカードが出てきます。この中には電子署名の

ためのPKIとオンライン認証のためのPKIの2つが入っています。この新行政カードは、今の住基カードのタイプ2になります。このカードは、基本的に電子パスポートと同じものなので、電子パスポートの中に入っている情報をこのカードに書き込むと、近いうちにできる成田等の出入国の自動化ゲートでも使えます。パスポートの代わりに、このカードでも出入国ができるようになるかは別の議論が必要ですが、一方では、身分証明でＥＵ圏内を移動できることを考えると、大きな利便性を提供する可能性もあります。アジアの中で日本がリーダーシップをとるのであれば、まさしくこのような手段で韓国やシンガポール、タイ等へ行けるようにするのも面白いと思います。

次に保険証としての利用法の案を説明します。カードをお持ちの住民の方は、はじめに入っている健康保険組合に申請します。健康保険組合は組合のデータベースと突合して、カードと保険証番号との紐付けを行います。この方法ですとカードの中には何も追加しないので、カードの取り扱いは非常に楽になります。このカードを持って医療機関に行くと、医療機関の受付からオンライン認証の機能を使って、資格確認を行います。これで先ほど述べた500万件の返戻はなくなると期待されます。これだけでも効果があることは明らかです。もちろん360万件ある転記ミスもなくなります。こういった積み重ねが重要なのです。

次には保険組合が変わるとき、および証明書が変わるときの対応が書いてありますが、時間の関係で説明を省きます。

ここまでの例では保険証そのものの情報をカードに記録していません。これは社会保障サービスがオンライン化されていることを前提としています。現実的には、カードが一たび普及した後に新しいサービスを追加する手間を省く手法になっていますが、一方では、オフラインしか使えないところが残ることも考えられます。このような場合には、保険証そのものを電子的な証明書にすることも考えられます。この場合には、カードに電子的な保険証をカードに書き込むことになります。この件については今後の議論が必要になると思います。このやり方の欠点は、カード内に証明書を記録するので容量が大きくなること等があげられます。

今のような背景を考えると、住基カードとeIDの整理することが必要になります。言うまでもなく、自治体の努力によって住基カードが普及しつつあります。このことには、深く敬意を表したいと思います。電子政府、社会保障サービス等の集約化が必要なことは明白です。

一方、ePassportの機能をカードが持つ可能性についても指摘しました。さらに、被災者に対する支援方策としても、このようなカードが有効であることも分かっています。例えば支援金を払うときの本人確認に有効でしょう。これらのことを総合して考えると、国による発行、券面統一、普及策の導入、国ができなれば、少なくとも都道府県クラスが行うべきであると思います。総務省さん、厚生労働省さんが主として関係するので、さらに関係省庁連絡会議の設置が必要になるでしょう。どのような形でどう動けるかはまだ分かりませんが、社会的な背景は整いつつあると思います。

まとめ

最後にまとめます。

医療分野の情報化を積極的に推進すべきです。電子政府・電子自治体の構築は、公的分野を含むべきで、決して中央政府や自治体だけの問題ではありません。さらに、既存の業務プロセスを見直し、事務経費の削減、IT投資の原資の確保、全体最適化などを実施すべきと考えます。

少々時間を超えましたが、私のプレゼンは以上です。これからのパネルディスカッションのための前振りなので、詳細についてはこの後のパネルディスカッションで議論させていただければと思います。以上で私の話を終了いたします。どうもご清聴ありがとうございました。

PART 1
COVER STORY

政府が掲げるIT戦略は、“正しい方向”を向いているか

“国家IT戦略”から“IT化の時代”を正しく読み解く

2001年に政府が打ち出した「e-Japan戦略」は、欧米諸国に対して後れを取っていた日本のIT活用を再び世界のトップレベルに押し上げようというビジョンを掲げたことで、大きな注目を集めた。しかしながら、同戦略の後を受けて、現在推進されている「IT新改革戦略」については、なぜかあまり話題に上ることがない。政府の取り組みは、IT産業の行方のみならず、一般企業のIT調達・運用戦略に少なからぬ影響を及ぼすものである。よって、企業のCIOも、その内容について、無関心でいるわけにはいかない。そこで本稿では、IT新改革戦略の概要を紹介するとともに、政府が進めようとしているIT戦略の方向性を展望する。

“基盤整備”から“活用”へ
——政府が示した“ITの5カ年計画”

まさに21世紀の幕が開けた2001年1月、「5年以内に世界最先端のIT国家になる」ことを目標に掲げて登場した政府の「e-Japan戦略」。その具体的な成果についてはさまざまな見方があるものの、ブロードバンド・ネットワークの整備や高機能携帯電話の普及、電子商取引の環境整備など、少なくともインフラの整備については、一定の成果を上げたとの意見が支配的だ。

また、政府自らが「IT」を重視する姿勢を明確に打ち出したことで、企業経営におけるITの重要性があらためて認識されるようになるなど、波及効果も少なくなかったと言える。

とはいえ、積み残された課題もけっこうある。それも、行政サービスや医療現場、教育現場などでのIT利用、地域あるいは世代の間での情報活用格差（いわゆるデジタル・デバイド）の是正、情報セキュリティ対策や防災対策の促進、国内IT産業の国際競争力の強化等々、いずれも、一筋縄で解決できるようなものではない。しかしながら、「最先端のIT国家」を目指すのであれば決して避けて通ることのできない重要課題ばかりである。

そんな“e-Japan戦略後”を見据えるかたちで、政府が2006年に新たな5カ年計画として発表したのが、2010年度を目標に「いつでも、どこでも、だれでもITの恩恵を実感できる社会の実現」を目標に掲げた、「IT新改革戦略」である。同戦略では、e-Japan戦略によってIT基盤の整備が進んだことを背景に、「我が国が取り組むべき喫緊の課題である構造改革を押し進めるためには、ITの有する構造改革力の追求が必要である」との理念をうたいあげている。つまり、「整備の時代は終わった。今後はITの持つ力を各分野の“改革”に生かしたい」というわけである。

その一方で、戦略の舵取りを担う組織体制については、e-Japan時代の枠組みが継承されている。縦割りの行政組織を束ね、府省横断・分野横断的な問題に取り組むための“推進役”を担うのは、e-Japan時代と同様、「高度情報通信ネットワーク社会推進戦略本部（以下、IT戦略本部）」である。同本部には、内閣総理大臣を本部長に、各国務大臣、民間企業の経営者、学識経験者らがメンバーとして名を連ねている。

1990年代から一貫してIT政策に携わり、IT戦略本部のメンバーをも務める東京工業大学教授の大山永昭氏は、IT新改革戦略のねらいについて、次のように語る。

「やはりIT新改革戦略の冒頭で掲げられている『いつでも、どこでも、だれでもITの恩恵を実感できる社会の実現』というのが最大の目標だ。医療、年金にまつわる行政手続きなど、ITを使えば、さらなる構造改革を進められる余地が十分にある。その意味では、IT新改革戦略は、e-Japan戦略から確実に一歩前進したものだと言える」

また、IT新改革戦略に関する政府の取り組み状況を評価し、他国との比較や新施策の提案を行うために、民間有識者などによって構成される「評価専門調査会」も設けられている。評価専門調査会の評価結果を今後策定される計画に適切に反映させることによって、PDCAサイクルを回すことを可能とし、方向修正が必要なものについては直ちに修正するという好循環を実